IDA PAPER P-2959

ATCCIS WORKING PAPER 25, EDITION 4

TECHNICAL STANDARDS FOR COMMAND AND CONTROL INFORMATION SYSTEMS (CCISs) AND INFORMATION TECHNOLOGY

T. F. Maggelet, *Project Leader*
R. P. Walker, *Principal Author*
R. P. Morton, *Project Leader*
S. H. Nash, *Principal Author*
P. B. Greer, *Editor*

February 1994

Prepared for
Office of the Assistant Secretary of Defense (C3I)
(Theater and Tactical Command, Control and Communications)

Office of the Director of Information Systems for C4,
Headquarters, Department of the Army
and
Office of the Director, Center for Standards,
Joint Interoperability and Engineering Organization,
Defense Information Systems Agency

INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street, Alexandria, Virginia 22311-1772

DEFINITIONS

IDA publishes the following documents to report the results of its work.

Reports

Reports are the most authoritative and most carefully considered products IDA publishes. They normally embody results of major projects which (a) have a direct bearing on decisions affecting major programs, (b) address issues of significant concern to the Executive Branch, the Congress and/or the public, or (c) address issues that have significant economic implications. IDA Reports are reviewed by outside panels of experts to ensure their high quality and relevance to the problems studied, and they are released by the President of IDA.

Group Reports

Group Reports record the findings and results of IDA established working groups and panels composed of senior individuals addressing major issues which otherwise would be the subject of an IDA Report. IDA Group Reports are reviewed by the senior individuals responsible for the project and others as selected by IDA to ensure their high quality and relevance to the problems studied, and are released by the President of IDA.

Papers

Papers, also authoritative and carefully considered products of IDA, address studies that are narrower in scope than those covered in Reports. IDA Papers are reviewed to ensure that they meet the high standards expected of refereed papers in professional journals or formal Agency reports.

Documents

IDA Documents are used for the convenience of the sponsors or the analysts (a) to record substantive work done in quick reaction studies, (b) to record the proceedings of conferences and meetings, (c) to make available preliminary and tentative results of analyses, (d) to record data developed in the course of an investigation, or (e) to forward information that is essentially unanalyzed and unevaluated. The review of IDA Documents is suited to their content and intended use.

The work reported in this document was conducted under contract MDA 903 89 C 0003 for the Department of Defense. The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of that Agency.

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-3040

COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

6 May 1994

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Technical Standards for Command and Control Information Systems (CCIS's) and Information Technology, IDA Paper 2959, February 1994

The Institute for Defense Analyses (IDA) has completed a review of technical standards applicable to future information technology. While the scope of the IDA effort was tactical command and control for the Year 2000 and beyond, this work has potential interest for many other types of defense information systems as well. The IDA paper provides an in-depth review of international and national, civil and military data communications and information systems standards that could be used to achieve interoperability, portability, and common operating environments. This work supports OSD efforts to promote the use of civil standards, including the Technical Architecture Framework for Information Management (TAFIM), to achieve open systems environments.

Attached is a copy of the standards analysis that has been completed under my direction by the DISA/JIEO Center for Standards and the U.S. Army. Questions and requests for additional information, including electronic copies can be directed to Dr. Robert P. Walker ((703) 845-2462 (e-mail rwalker@ida.org).

Richard G. Howe

Richard G. Howe
Director, Theater & Tactical C3

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
February 1994

3. REPORT TYPE AND DATES COVERED
Final

4. TITLE AND SUBTITLE
TECHNICAL STANDARDS FOR COMMAND AND CONTROL INFORMATION SYSTEMS (CCISs) AND INFORMATION TECHNOLOGY

5. FUNDING NUMBERS
MDA 903 89-C-0003

T-J1-246
T-S5-1211

6. AUTHOR(S)
Robert P. Walker, Theodore F. Maggelet, Paula B. Greer, Kevin J. Saeger, Sarah H. Nash, David A. Arthur, Edward A. Feustel, Richard P. Morton, Asghar I. Noor, Christine Youngblut

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
INSTITUTE FOR DEFENSE ANALYSES
1801 N. Beauregard Street
Alexandria, VA 22311

8. PERFORMING ORGANIZATION REPORT NUMBER
IDA PAPER P-2959

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

ASD (C3I)
Room 3D174, The Pentagon
Washington, DC 20301

Director, FFRDC Programs
1801 N. Beauregard Street
Alexandria, VA 22311

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
ATCCIS Working Paper 25, Edition 4

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This document is a joint effort between JIEO, OSD, and the US Army. It is a major revision of Technical Standards for Command and Control Information Systems, ATCCIS Working Paper 25 (WP 25), Edition 3, January 1992, and of the update to the above document, IDA Paper P-2805 (Volumes I and II), December 1992, prepared for JIEO. The focus remains the identification of open standards that could be used to achieve interoperability of command and control information systems (CCISs), but the document is applicable to a wide range of information systems and information technology activities. This document has had significant contributions from NATO organizations and national staffs; SHAPE; and, in the United States, the Services, JIEO, and other organizations.

This document has been reorganized and extended to be aligned with the Technical Reference Model contained in Edition 2.0 of the US DoD Technical Architecture Framework for Information Management. The document places increased emphasis on the use of profiles to achieve interoperability.

14. SUBJECT TERMS
DoD, Information Technology (IT), IT Standards, Tactical Command and Control, Interoperability, NATO, SHAPE, Army Tactical Command and Control Information Systems (ATCCIS), Open Systems, Open Systems Interconnection (OSI), Portability, Standards, Profiles, GOSIP, Stacks, Options, Assessment, Data Communications, Data Transmission, Architectures, Reference Models, Software Engineering Services, User Interface Services, Data Management Services, Data Interchange Services, Graphics Services, Network Services, Operating System Services, Security Services, System Management Services, Distributed Computing Services, Internationalization Services, Technical Standards, Application Interfaces, POSIX, TAFIM.

15. NUMBER OF PAGES
887

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	Same as Report

UNCLASSIFIED

IDA PAPER P-2959

ATCCIS WORKING PAPER 25, EDITION 4

TECHNICAL STANDARDS FOR COMMAND AND CONTROL INFORMATION SYSTEMS (CCISs) AND INFORMATION TECHNOLOGY

T. F. Maggelet, *Project Leader*
R. P. Walker, *Principal Author*
P. B. Greer, *Editor*
D. A. Arthur
K. J. Saeger

R. P. Morton, *Project Leader*
S. H. Nash, *Principal Author*
E. A. Feustel
A. I. Noor
C. Youngblut

February 1994

Approved for public release; distribution unlimited.

INSTITUTE FOR DEFENSE ANALYSES

Contract MDA 903 89 C 0003
Task T-J1-246
Task T-S5-1211

UNCLASSIFIED

FOREWORD

The purpose of this paper is to make available substantive work done in response to a major cooperative technical support activity among agencies in the US and many NATO nations. Specifically, this paper was prepared[1] by the Institute for Defense Analyses (IDA) in support of the Supreme Headquarters Allied Powers Europe (SHAPE)-sponsored Army Tactical Command and Control Information System (ATCCIS) Phase III study effort and the Defense Information Systems Agency (DISA), Joint Interoperability and Engineering Organization (JIEO), Center for Standards. The contents of this document were reviewed and agreed to in the international ATCCIS forum, and issued by SHAPE as a NATO UNCLASSIFIED document with the same title. It was also reviewed by the Center for Standards, Directorate for DoD Standards Assistance. Comments from NATO and national commands and agencies were solicited and have been incorporated. SHAPE will be distributing this paper to all NATO nations and to those NATO commands and agencies that have expressed an interest in the ATCCIS study. Additional distributions are planned by the ATCCIS nations, NATO Headquarters (to the TSGCE), and NACISC (to the Information Systems Working Group). Background information relating to the overall ATCCIS effort is contained in the Preface to this paper.

This document is a joint effort between JIEO, OSD, and the US Army. It is a major revision of *Technical Standards for Command and Control Information Systems,* ATCCIS Working Paper 25 (WP 25), Edition 3, January 1992, and of the update to the above document, IDA Paper P-2805 (Volumes I and II), December 1992, prepared for JIEO. The focus remains the identification of open standards that could be used to achieve interoperability of command and control information systems (CCISs), but the document is applicable to a wide range of information systems and information technology activities. This document has had significant contributions from NATO organizations and national staffs; SHAPE; and, in the United States, the Services, JIEO, and other organizations.

This document has been reorganized and extended to be aligned with the Technical Reference Model contained in Edition 2.0 of the US DoD *Technical Architecture Framework for Information Management.* The document places increased emphasis on the use of profiles to achieve interoperability.

The Office of the Director of Information Systems for Command, Control, Communications and Computers (ODISC4), Headquarters Department of the Army, provides the US delegate to the ATCCIS Permanent Working Group (PWG), representing SHAPE, Allied Forces Central Europe (AFCENT), SHAPE Technical Centre, Denmark, France, Germany, the Netherlands, Spain, the United Kingdom, and the United States. Within the United States, operational issues are coordinated with the US Army Training and Doctrine Command. Technical issues are coordinated with the US Army Space and Strategic Defense Command and the US Army Communications-Electronics Command. IDA provides technical and analytical expertise in support of the US contributions to the overall ATCCIS effort. ODISC4 also furnishes the U.S.

1 This document was prepared in response to requests from the Office of the Assistant Secretary of Defense (C3I), Theater and Tactical Command, Control, and Communications under Contract MDA903-89-C-0003, Task Order T-J1-246, and the Joint Interoperability and Engineering Organization (JIEO), Defense Information Systems Agency (DISA), Task Order T-S5-1211. Funding for Task T-J1-246 was provided by the US Army Office of the Director of Information Systems for Command, Control, Computers, and Communications (DISC4).

delegate to the ATCCIS Steering Group, which provides overall direction and approval of the ATCCIS PWG work effort. This document should be of primary interest to the combat development and system development communities of those US Commands and Agencies whose focus is on longer term command and control requirements (i.e., the year 2000 and beyond).

The authors would like to acknowledge the following persons for contributions and comments on standards and examples of military initiatives to use open standards: Mr. Nelson Alvarez (DISA/JIEO), LTC Dan Almero (US Army, Vice-Chair, WG3 on Land Operations, ADSIA), LCDR Katie Bryant (DISA/JIEO), LCDR David Chappell (DISA/JIEO), Mr. Walt Claasen (LOGICON), Dr. Frank Curcio (DISA/JIEO), Mr. Silvano Goldoni (NACISA), CDR Tony Hunt (UK Royal Navy, SHAPE), Mr. Wouter Konings (ISWG/NACISC), Mr. David Lambert (BICES Team), MAJ Michael Mascarenas (USMC), Mr. Richard McLane (DISA/JIEO), Mr. Salvatore Manno (DISA/JIEO), Mr. Joseph Onufer (US Army CECOM), Mr. Henry Saphow (OPM FATDS, US Army), Mr. Stan Levine (OPM CHS, US Army), Dr. A. Rannestad (NATO International Staff), Ms. Judy Simpson (LOGICON/Eagle Technologies), Mr. Hal Staton (NSA), and Ms. Christina Vicini (NACMA). The substantial technical support of the sponsors, Mr. Vic Russell [OASD(C3I)-T&TC3] and LCDR Doug Schroeder (DISA/JIEO), as well as the US Representative to ATCCIS, LTC Steve Woffinden (US Army ODISC4), is gratefully acknowledged.

PREFACE FOR ATCCIS

1. In 1978, NATO's Long Term Defence Plan (LTDP) Task Force on Command and Control (C2) recommended that an analysis be undertaken to determine if the future tactical Automatic Data Processing (ADP) requirements of the Nations, including interoperability, could be obtained at a significantly reduced cost when compared with the approach that had been adopted in the past. The Task Force also recommended that the analysis should determine whether tactical ADP systems could be developed according to technical standards prescribed by NATO and agreed upon by the Nations.

2. In early 1980 the then Deputy Supreme Allied Commander Europe initiated a study to investigate the possibilities of implementing the Task Force's recommendations. Three Nations, those with experience in fielding automated tactical command and control information systems, participated in Phase I of the study, with Supreme Headquarters Allied Powers Europe (SHAPE) as leader and coordinator. The study group reported, at the end of Phase I, that the Nations could increase interoperability and potentially reduce costs by using a common development approach.

3. The Army Tactical Command and Control Information System (ATCCIS) Phase II study, under the direction of a steering group chaired by SHAPE and consisting of representatives from the Central Region (CR) Nations and Allied Forces Central Europe (AFCENT), was established in 1984. Concurrently, a permanent working group (PWG) was formed which consisted of military, technical, and analytical representatives from France, Germany, the United Kingdom, the United States, SHAPE and AFCENT, and technical support from SHAPE Technical Centre (STC) to progress the Phase II effort. That effort commenced in January 1985 and finished in October 1990; it recommended that all NATO Nations, as well as the Allied Command Europe (ACE) Northern and Southern Regions, be invited to participate in a Phase III effort.

4. ATCCIS Phase III has the aim of demonstrating the ATCCIS architecture and operational requirements in a multi-national scenario with each participating nation fielding ATCCIS conformant systems. The demonstration phase, sponsored by SHAPE, commenced in January 1992. As of July 1993, three additional nations had agreed to participate in ATCCIS as full participating members, i.e., the Netherlands, Denmark and Spain, with three nations observing, i.e., Belgium, Canada and Italy. The work of the PWG supports the Military Agency for Standardization (MAS) Army Board (AB) initiative to modernize critical C2-related STANAGs; additionally, it will harmonize its work with the Allied Data Systems Interoperability Agency (ADSIA) and will maintain links with the Allied Tactical Communications Agency (ATCA) to ensure that no duplication of effort occurs. The PWG also coordinates its activities with the Tri-Service Group on Communications and Electronics (TSGCE).

(This page intentionally left blank)

CONTENTS

LIST OF FIGURES

LIST OF TABLES

TECHNICAL STANDARDS FOR COMMAND AND CONTROL INFORMATION SYSTEMS (CCISs) AND INFORMATION TECHNOLOGY

1. INTRODUCTION

1.1 Derivation

This paper originally derived from the Phase II Working Paper (WP) 24 [Ref. ATCCIS 1988], which defines the basic concepts, logical elements (called facilities), and attributes of the architecture for the Army Tactical Command and Control Information System (ATCCIS), a common army command and control system concept for the year 2000 and beyond. The objectives of the ATCCIS architecture are to achieve interoperability through common standards and maintain the potential to reduce costs of future command, control, and information systems (CCISs), without unnecessarily restricting national options for implementation. The paper has been recently reorganized and extended to be consistent with the POSIX Open Systems Environment (OSE) Reference Model (P1003.0) developed by the Institute of Electrical and Electronics Engineers (IEEE) [Ref. IEEE 1993] and is now applicable and useful for all defense information systems.

1.2 Purpose

The purpose of this paper is to identify the technical standards that are applicable to automated information systems (AISs), including CCISs. These systems are defined to be a combination of information, computers, and telecommunications resources and other information technology, together with personnel resources, that collect, record, process, store, communicate, retrieve, and display information [Ref. DoD 7920.2 1990]

This paper identifies standards that can be used to define implementations of information systems. In this paper, existing and planned standards appropriate to the 11 service areas common to most AISs are surveyed to the level of detail necessary to confirm a reasonable basis for the future support of the CCIS requirements. Relevant standards are identified, but no recommendations for selecting standards are considered. Gaps in current and planned standards coverage, which may require some developmental effort, are identified and are being passed to the appropriate standards defining bodies, including those within NATO. This document also offers guidance in ensuring adequate coverage by the set of standards employed at the time of implementation.

It is not yet known to what degree international commercial standards can be made to satisfy CCIS requirements, but it is assumed that the extraordinary investments in open system standards during the 1980s and 1990s could have a major impact on the next generation of CCISs. As the nations explore the use of these standards in their military and non-military systems, many of the practical issues not addressed in this paper will be resolved.

1.3 Scope

This working paper presents information and analyses that are intended to support defense AISs, with particular emphasis on the exchange of data that preserves the meaning and relationships of the data exchanged (termed "basic interoperability").

This paper contains information on existing and planned international, voluntary, government, and de facto standards that promote interoperability and portability, ensure flexibility and growth potential, and allow for technology insertion through use of commercial off-the-shelf (COTS) products and nondevelopmental items (NDIs). The paper identifies relevant standards and gaps in current and planned standards coverage that may require development effort. It does not, however, provide a detailed evaluation of the standards, but instead focuses on standards activities leading to future standards as well as the current issues surrounding these activities.

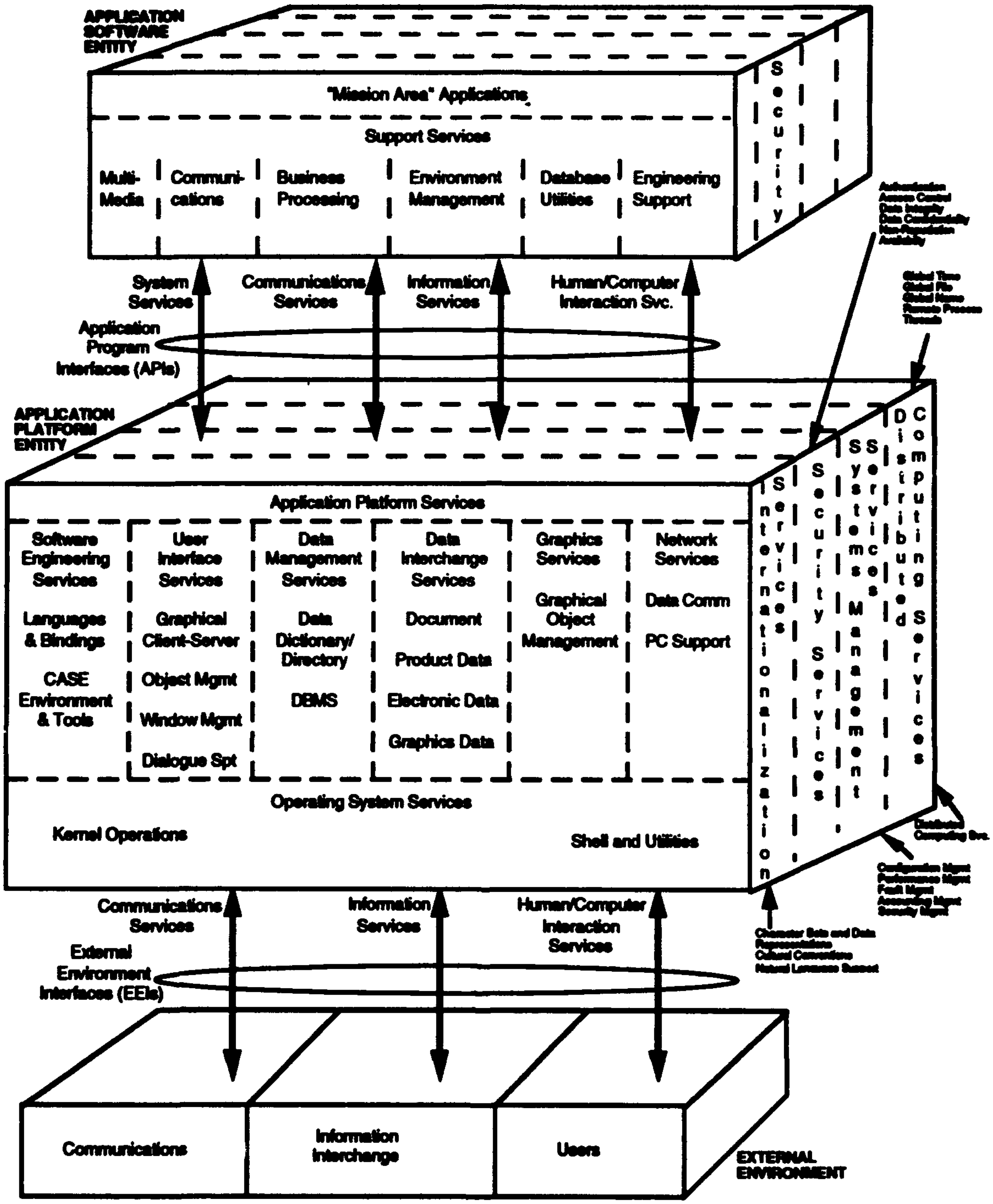
This paper provides a broad overview of the existing and developing technical standards applicable to AISs, to include automated CCISs. Very little of the work is specific to tactical CCISs. The standards are applicable to many types of information systems and have been the attention of many national and international efforts to reduce acquisition costs of government- and industry-procured systems.

The scope of the analysis of standards, which is the focal point of this paper, is broad, extending to international and national, commercial and military standards. However, the emphasis is on international commercial standards with military enhancements where required.

The technical scope is intended to match that of the application platform services described in the current version of the Technical Reference Model (TRM) [Ref. TAFIM 1993, Volume 2], depicted in Figure 1, which is a modification of P1003.0, the POSIX OSE Reference Model and which, in turn, is the basis for the NATO Open Systems Environment (OSE) Reference Model [Ref. NATO OSE 1993]. Substantial new material has been added to this document in areas such as distributed system services, object management, lower-layer network services, security, and system management.

1.4 Information Sources

This assessment is based primarily on a review of standards for open systems developed by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the International Telecommunications Union (ITU) - Telecommunication Standardization Sector (ITU-TS) [formerly the International Telegraph and Telephone Consultative Committee (CCITT)]. Since ISO/IEC has decided to use the profiles of standards being developed by regional standards workshops, the primary sources for profiles are those workshops. Use of open systems standards in the North Atlantic Treaty Organization (NATO) is the responsibility of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 (SG9) on Data Distribution; thus, TSGCE SG9 draft Standardization Agreements (STANAGs), the draft *NATO Open Systems Interconnection Profile (NOSIP) Strategy* [Ref. NATO 1993a], *NATO Technical Interoperability Standards (NTIS) Transition Strategy* [Ref. NATO 1991], and working documents from international and national sources form the basis of the assessment of military use of open systems standards.



Sources: POSIX 0 [Ref. IEEE 1993] and US DoD Technical Reference Model [Ref. TAFIM 1993, Volume 2].

Figure 1. Example Technical Reference Model

Access to many of the key documents has been the result of the contributions of experts from many nations and from maintaining active membership in the Open Software Foundation

(OSF), the Object Management Group (OMG), and the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X3T5.[1]

The cut-off date for information contained in this paper is February 1994. The primary effect of the cut-off date is that the progression of some standards to committee draft (CD), draft international standard (DIS), and international standard (IS or ISO) status may not be fully reflected herein.[2]

1.5 Methodology for ATCCIS Standards Analysis

This section describes the methodology employed to identify the group of existing and planned standards required to support required system functionality (for AISs, CCISs, or specifically ATCCIS) and to assess the completeness of standards coverage. The methodology is illustrated in Figure 2.

The ATCCIS architecture will be defined by adopting existing or emerging standards wherever and whenever possible. Further, when such a standard cannot be found ATCCIS will identify the requirement for a standard to be developed and will pass such a requirement to the appropriate standards defining body within NATO. Each facility in the ATCCIS architecture is a logical entity that provides a set of related services; implementation of a facility is not defined by the architecture and is a national responsibility for each system. This paper identifies standards (and options within standards) that are applicable to each facility, but the paper does not recommend specific standards or groups of standards. Selection of appropriate standards, as well as the basic design choices implicit in the standards and options within standards, will be made by agreement prior to implementation decisions.

Following a review of the required services, the next step is to identify the base standards appropriate for each group of services. These standards may come from international, NATO, national military, or national non-military standards bodies, and they may be existing or planned. High-level options within standards applicable to CCISs are identified. (Sources and the development process for international standards are discussed in Chapter 3.)

For many functions, there are several interrelated standards that must be used together to provide the required services. In most cases there is an order or hierarchy among these standards in which the lower levels are closer to physical means, and higher levels are associated with applications that are independent of the physical means. An ordered grouping of standards is called a stack. A profile is a stack of standards for which the interoperability parameters are partially or fully specified (profiles usually represent agreements among implementors). Where applicable to services required by CCISs, stacks will be constructed and illustrated in tables or figures.

Assurance of adequate standards coverage is addressed in three ways. First, WP 25 checks for the existence of standards that generally support each specific ATCCIS function. Requirements for which no existing or planned standard seems to exist, or for which existing

1 Accredited Standards Committees such as X3T5 operate under the procedures of ANSI and are technically not part of ANSI; nevertheless, in this document, ANSI ASC X3T5 is abbreviated as ANSI X3T5.

2 Significant contributions have been received from representatives to TSGCE, the UK Defence Research Agency (DRA), the American National Standards Institute (ANSI), the US National Institute of Standards and Technology (NIST), the US Defense Information Systems Agency (Joint Interoperability and Engineering Organization), the Open Software Foundation (OSF), Omnicom, and Technology Appraisals (UK).

standards do not seem to be adequate, are identified so that these needs may be referred to the appropriate NATO standards defining body.

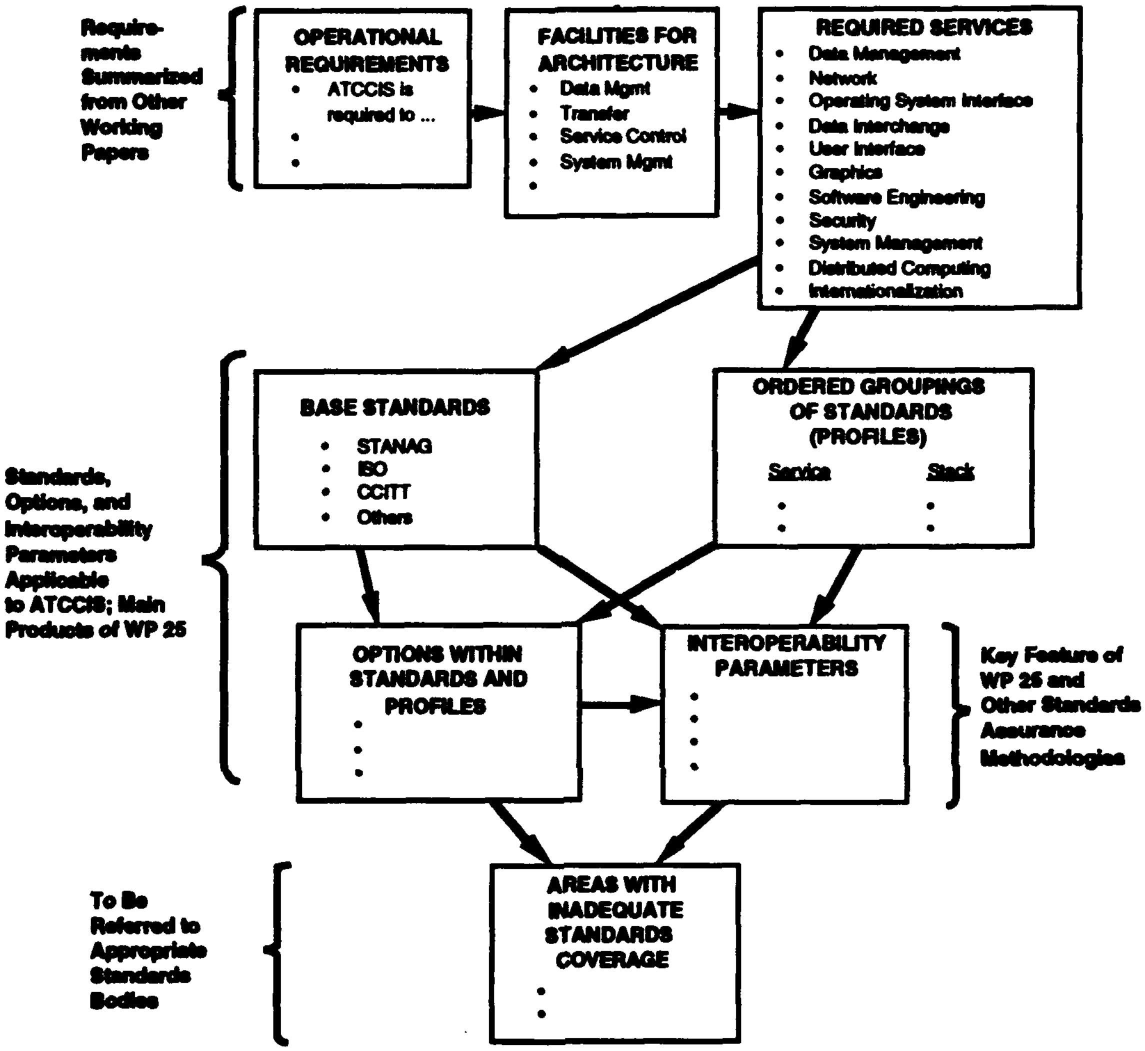


Figure 2. Overview of the Methodology for ATCCIS Standards Analysis

On a more specific level, a methodology for ensuring adequate standards coverage through detailed analysis has been developed. An interoperability parameter approach is defined that begins with the identification of the system design parameters whose control is required to achieve interoperability. The assembled parameters act as a checklist for interoperability since each interoperability parameter must be controlled by a suitable standard. The purpose of an analysis using interoperability parameters is to recognize and examine all relevant quantities and characteristics in a direct manner, instead of assuming that existing or draft standards will provide adequate coverage of the quantities. Appendix B discusses this approach in more detail. NATO's TSGCE SG9 and ISO/IEC have developed a format, called a standardized profile, for specifying stacks and interoperability parameters. Standardized profiles are discussed in Chapter 16, and

examples are provided in Appendix I. The status of NATO work to address military deficiencies in open system standards (primarily for network services) is given in Chapter 17.

In the third step of the coverage analysis, the array of standards identified that could support ATCCIS is compared with plans for near-term efforts to check for completeness. Near-term efforts include: developing NATO C2 systems, such as the Air Command and Control System (ACCS); and conducting multilateral interoperability demonstrations, such as the Quadrilateral Interoperability Programme—these are discussed in Chapter 18. National initiatives for military use of OSI standards are reviewed in Chapter 19, and detailed examples are given in Appendix C. In addition to providing a check on completeness of ATCCIS applicable standards, some of these near-term efforts are of interest because they represent transition strategies for moving to open environments for information processing and exchange.

1.6 Structure of the Paper

Figure 3 identifies the roles of each of the chapters. Chapter 2 provides an overview of the standardization process and is essential to understanding the assessment. Chapter 3 provides background on architectures, frameworks, and reference models. The remaining chapters are generally independent and can be read in any order. Chapters 4 to 14 address the 11 service areas shown in Figure 1 (above): software engineering, user interface, data management, data interchange, graphics, network, operating system, security, system management, distributed computing, and internationalization. Chapter 15 describes the interface standards essential to ensuring that applications entities are, to the extent possible, independent of hardware. Chapter 16 summarizes international and national activities to develop profiles of standards in order to ensure common sets of interoperability parameters are selected for acquisition. The work in NATO and national military organizations to adopt, modify, and implement open systems standards is reviewed in Chapters 17-19. Chapter 20 summarizes the issues uncovered in the previous chapters.

Several appendixes, some lengthy, are provided as reference material. Appendix B expands the discussion of the interoperability parameter methodology and applies the approach to some commonly used standards (RS-232, RS-423, STANAG 4202, and ITU-TS X.25). Appendix C provides examples of profiles of national initiatives to address the military use of OSI standards. A compilation of technical standards being developed by ISO and ITU-TS is given in Appendixes D and E, the former listed by layer of the OSI Reference Model and the latter listed numerically. Appendix F identifies the role and (in some cases) the standards responsibility of international and national, both civil and military, standards bodies. Appendix G provides some detailed information on the work plans for one of the major subcommittees (SC21) ISO/IEC (JTC1). Appendix H identifies STANAGs and other military and commercial standards being developed for use in open systems. Appendix I summarizes the application, transport, and relay functional profiles identified for use in NATO. Appendix J identifies the status of and the military features contained in the open systems interconnection (OSI) STANAGs being developed by the TSGCE. An index is provided to assist the reader in locating information on specific topics and standards.

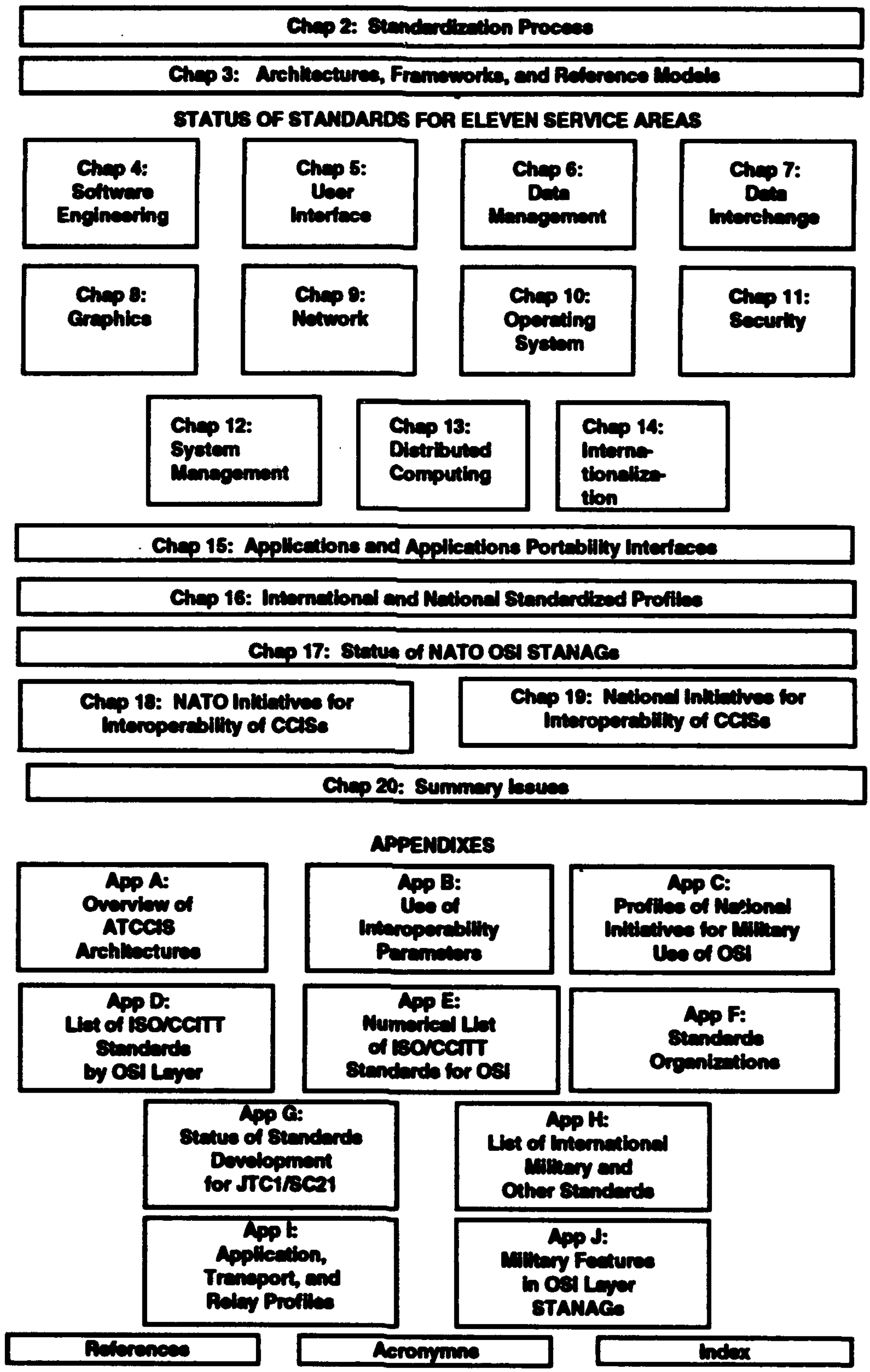


Figure 3. Organization of Document

(This page intentionally left blank)

2. STANDARDIZATION PROCESS

2.1 Goals for Information System Standards

The desire to adopt standards that govern various aspects of information system definition derives from the following goals:

- To save money by separating software from hardware. The rapid rate of change in computer hardware technology and declining prices makes it desirable to be able to replace hardware and hardware vendors without having to rebuild software. Standards that govern the interfaces between application software and system software limit the scope of such changes to those portions of the system software that manage the hardware.
- To save money by promoting competition among component vendors. The existence of open, non-proprietary standard specifications for a component of an automated information system, either hardware or software, creates a market in which multiple vendors can compete. When the specifications are owned by one vendor, they can lock out competition for after-market components, locking in the user to the software offered by the hardware vendor.
- To facilitate the adoption of new technology. The same arguments that apply to saving money also apply to adopting new hardware and software technology. In this case, however, part of the advantage of having standards stems from the architectural structure imposed by the process of grouping the standards into service areas. This isolates the impact of new technology to only that portion of a system directly affected by the change. For example, the adoption of voice recognition systems would only impact the user interface component of the platform, and could be isolated from existing applications while permitting new applications to take better advantage of the new capabilities.
- To promote operational effectiveness through interoperability between systems belonging to different organizations, or even between systems of the same organization. Interoperable systems are ones that can exchange data in ways that preserve the meaning of the data. This permits users with the appropriate permissions to access data not previously available to them or in a more convenient way. This, in turn, allows them to work more effectively, more efficiently, or both.
- To promote workplace efficiency through the integration of information systems. Integration goes beyond interoperability to make applications aware of other applications, not just data. Integrated applications offer the potential for better integrated organizations, and the potential for substantial cost savings in software development by sharing applications instead of rewriting them.

These goals, and the strategies they engender, strongly influence the standardization process within defense organizations, as well as in the world at large. For example, the intention of taking advantage of marketplace competition has spurred some nations into placing commercial standards ahead in priority of defense-unique standards. Similarly, the desire to more quickly incorporate new technology into standards faster is changing the procedures in use for the development and approval of proposed standards documents.

2.2 Categorization of Standards

Standards can be categorized in several ways. One is by content: interface, process, or product standards. Interface standards are the least restrictive and merely define certain characteristics. Process standards, while somewhat more restrictive, define the manner in which a

process is performed, but do not determine the actual output. Product standards, since they define a particular output or outcome, tend to be the most restrictive. These categories also indicate the likely effects of a particular standard (or function of a standard) in terms of whether certain groups may resist the standard and how well the standard will be integrated into the technology life cycle. For example, a product standard promulgated too early in the technology life cycle may be resisted and not implemented by industry because it does not allow enough flexibility in adapting to anticipated changes in the technology. Conversely, simple interface standards may be insufficient for users or maintainers of a product who require accurate or detailed information about a particular product and how it functions. [Ref. Putnam 1982] Most of the standards described in this document are interface standards.

Two additional types of standards—reference models and profiles—represent an orthogonal categorization to interface, process, and produce standards. Reference models provide a common framework for a group of standards within a specific area. For example, the model shown in Figure 1 (above) establishes a very high level structure of all the standards of interest in the area of application platforms for AISs by dividing the platform into 11 substructures, many of which have their own reference models to provide further structure to their area.

Interface, process, and product standards frequently have many options. Profiles are defined to establish a common set of options so that the goals of interoperability and integration can be realized by implementations of the standard. Profiles have been developed from at least two different perspectives. One, represented by a national or NATO open system interconnection profile, provides both a selection of specific standards where there are alternatives, as well as some of the specific options within those standards. Others represent the very detailed specifications to be used by a specific community of users or for a specific purpose.

Another way to categorize standards is by issuing body. International standards are issued by an organization whose standards development process is accepted by the international community as being an open, consensus-based process. National standards are issued by similar organizations at the national level, usually with governmental backing. Industry standards are issued by an organization that provides an open process within a specific industrial area. Those may be professional societies, such as IEEE, or trade associations, such as the European Computer Manufacturers' Association (ECMA). Consortia standards are issued by representatives of groups of producers, consumers, and government bodies. In some cases, the standards development process may be open only to the members of the consortium. These different kinds of issuing bodies are layered to some degree. The members of the international organizations are the national standards bodies. Industry bodies and consortia frequently propose their standards for adoption by the national bodies, or sometimes directly to the international bodies. Thus, for example, an IEEE standard may be offered to ANSI as a US standard and, once accepted, offered to the International Organization for Standardization (ISO) as an international standard.

Two major characteristics distinguish the standards produced by these different issuing bodies: time for development and vendor acceptance. In general, the narrower the scope of consensus, the less time it takes to develop a standard. Consortia standards usually take the least amount of time, but if there are competing consortia within a single area, or if the membership is too limited, the result may not achieve the degree of vendor acceptance to make the standards de facto standards. On the other hand, international standards may take so long to develop that proprietary products become de facto standards and are very hard to dislodge in the marketplace.

An example of the latter is the suspension of development of ISO's Terminal Management (TM) standard in favor of standardizing the popular (de facto) X-Windows user interface.

2.3 Standards Organizations

This section describes selected standards organizations and the process used by each. The organizations described are:

- International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)
- International Telecommunications Union (ITU) Telecommunications Standardization Sector (ITU-TS)
- American National Standards Institute
- X/Open
- Tri-Service Group on Communications and Electronics (TSGCE)
- Regional organizations producing standardized profiles for adoption by ISO
- National defense organizations developing OSI profiles, such as the US Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP).

ISO. Development of an ISO standard, from first proposal to actual publication of the standard, is an arduous and time-consuming process that ensures the final result to be acceptable to as many countries as possible. Figure 4 is a flowchart of the process.

The process begins when a member body, often referred to as a national body (NB), submits a new work item (NWI) proposal (NP). The introductory proposal is assigned to a working group (WG) of a technical committee (TC) or subcommittee (SC), which will be responsible for progressing the document through the standardization process. In this initial stage, the proposal is called a working draft (WD). The appropriate WG of the assigned TC publishes the WD in the form of a committee draft (CD) [prior to February 1990, CD was known as a draft proposal (DP)]. The CD is then circulated among interested members for a 3-month balloting and comment period.

If the CD obtains substantial support, it is then circulated (with agreed changes) as a draft international standard (DIS) for a 6-month balloting period. If the DIS receives a majority approval by the TC members and 75 percent approval from all voting members, it is advanced to the Central Secretariat. If the balloting of the DIS is negative, the DIS text is revised by an editing committee and resubmitted as a second DIS for balloting or demoted to CD status for work to continue on building consensus. The Central Secretariat submits an approved DIS to the ISO Council, the board of directors of ISO. The council accepts the DIS as an international standard (IS),[3] and finally, ISO publishes the international standard.

A standard that has achieved DIS status is considered to be stable. Only minor changes are made to DIS text draft prior to becoming an international standard. If it is necessary to modify an existing or emerging standard, there is an addendum process whose steps are: working draft addendum (WDAD), proposed draft addendum (PDAD), draft addendum (DAD) with DIS status, and addendum (AD) with international standard status. A similar process [working draft amendment (WDAM), preliminary draft amendment (PDAM), draft amendment (DAM), and amendment (AM)] is used for amendments. In addition, technical corrigenda may be approved to

---

[3] ISO is used in this document to denote an international standard adopted by ISO or jointly by ISO/IEC.

correct technical errors that do not affect the intended standardization. A technical report (TR) is issued first as a working draft technical report (WDTR), then as a preliminary draft technical report (PDTR), and, when at DIS status, as a draft technical report (DTR).

A subcommittee of ISO/IEC's Joint Technical Committee One (JTC1) on Information Technology may suspend the five-stage process in favor of the fast track process, initiated by a national body or a Category A liaison organization, provided that the subcommittee agrees:

- That the intended fast track document is suitable to satisfy the requirements of the existing JTC1 project
- To use the fast track process and so notifies JTC1.

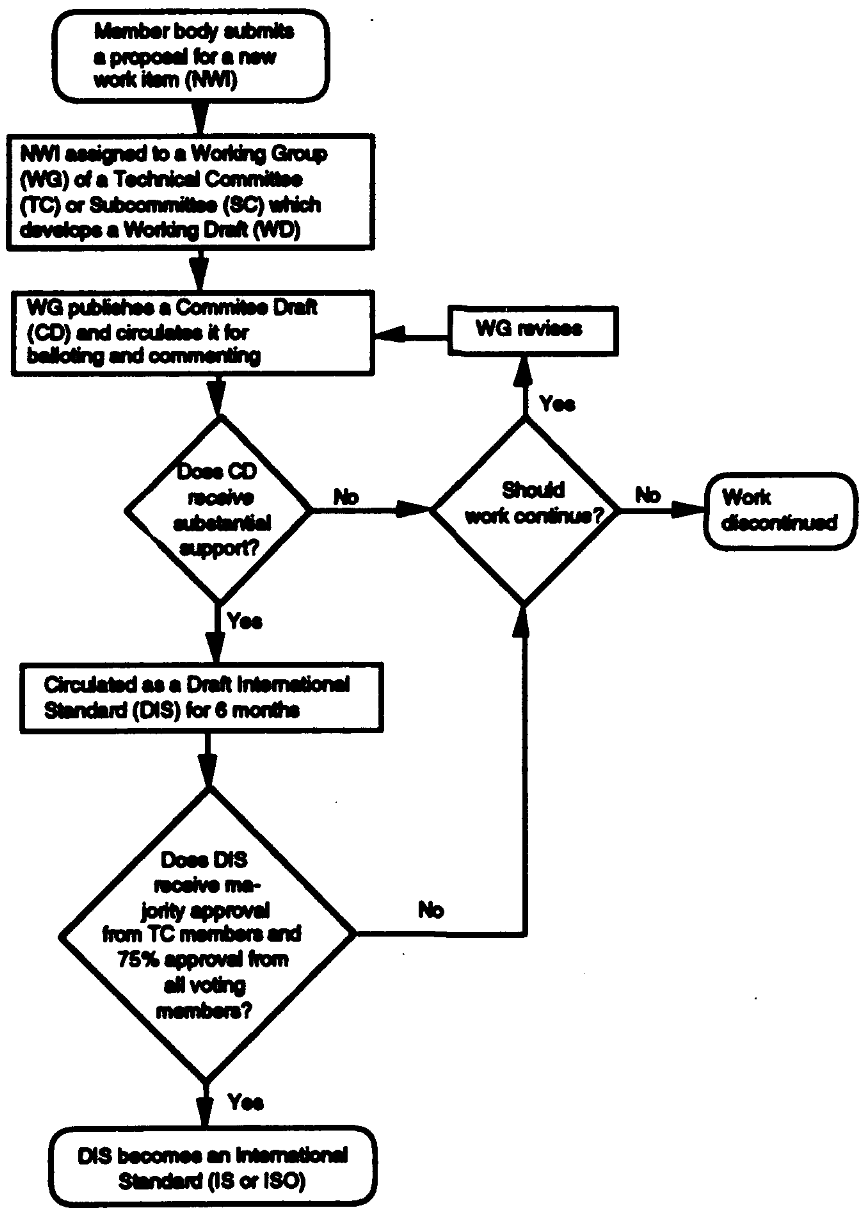


Figure 4. Flowchart of the ISO Standardization Process

At its March 1993 Plenary in Berlin, JTC1 requested that national bodies submit contributions on mechanisms for accelerating the 5-stage process, and additional expediting

procedures to accommodate other situations for which current processes may not be timely. At present, fast track candidates enter the ISO process as CDs for DIS balloting. [Ref. SC21 N 7713 1993]

The ISO/IEC JTC1 Special Group on Functional Standardization (SGFS) is developing standards for international standardized profiles (ISPs). As such, they bear an ISP prefix in lieu of the traditional ISO prefix although their numbers follow the ISO numerical sequence. Designations for drafts being refined for ISP status are pDISP for proposed draft ISP and DISP for draft ISP.

ISO/IEC. ISO/IEC is a voluntary, nontreaty organization that develops standards in many areas that facilitate the international exchange of goods and services. The members of ISO/IEC are organizations chosen by the participating nations and nonvoting, observer organizations. Most ISO/IEC members are government standards institutions or organizations incorporated by public law.[4]

ISO/IEC is organized, under the administrative arm of the Central Secretariat, as a group of technical committees chartered to produce standards in various areas. The committee :t relevant to this work is the JTC1 of ISO/IEC (formerly, TC97 on Information Processing Systems). JTC1 is organized into subcommittees and working groups that actually produce the standards. The work related to OSI is carried on by subcommittees SC6 (lower layers) and SC21 (upper layers). More specifically, the working groups of prime interest are:

- SC6—Telecommunications and Information Exchange Between Systems
  - WG1—Data Link Layer
  - WG2—Network Layer
  - WG3—Physical Layer
  - WG4—Transport Layer
  - WG5—Private Integrated Services Networking
- SC18—Text and Office Systems
- SC21—OSI, Data Management, and Open Distributed Processing
  - WG1—OSI Architecture
  - WG3—Database
  - WG4—OSI Management and OSI Directory
  - WG5—Specific Application Services and Protocols (now merged with WG6 into WG8)
  - WG6—Session, Presentation, Common Application Service Elements, and Upper Layer Architecture (now merged with WG5 into WG8)
  - WG7—Open Distributed Processing
  - WG8—OSI Upper Layers (formerly WG5 and WG6)
  - WG9—Testing
- SC22—Programming Languages
- SC27—Common Security Techniques for Information Technology Applications
  - WG1—Secret Key Algorithms and Applications
  - WG2—Public Key Cryptosystems and Modes of Use
  - WG3—Use of Encipherment Techniques in Communication Architectures.

4 For example, the member bodies from the FR, GE, UK, and US are the Association Francaise de Normalization (AFNOR), Deutsches Institute fur Normung (DIN), British Standards Institute (BSI), and American National Standards Institute (ANSI), respectively. Other member bodies are identified in Appendix F.

At its March 1993 Plenary in Berlin, JTC1 agreed to a revised title and scope of SC21. Formerly called Information Retrieval, Transfer, and Management for OSI, the new title is Open Systems Interconnection, Data Management and Open Distributed Processing. The new scope is as follows [Ref. SC21 N 7720 1993]:

- *Standardization of protocols, services, interfaces, and information objects, and of related reference models covering the areas of OSI; management of data and information resources in both local and distributed processing environment; open distributed processing; security and management aspects related to these areas; and the relationships among these areas.*
- *Standardization of related conformance testing methodologies, description languages and techniques, and registration procedures.*

Now that the fundamental lower layer standards developed by SC6 are in place, SC21 is the more active of the two subcommittees; a summary of the ongoing projects and expected completion dates of standards now in development is given in Appendix G. SC6 is active in security and management for the lower layers, as well as continuing work in standardization of new subnetwork technologies and interworking of subnetworks. SC18 works on document standards and SC22 works on programming language standards, while SC24 concentrates on computer graphics (discussed in Chapter 11). SC27 on Security Techniques is of interest to the security services discussed in Chapter 8. Standards from all these groups are included in the lists provided in Appendixes D and E. The detailed program of SC21 is summarized in Appendix G.[5]

ITU-TS. The ITU-TS [formerly the International Telephone and Telegraph Consultative Committee (CCITT) and International Radio Consultative Committee (CCIR)][6] is one of three sectors of the International Telecommunications Union (ITU), a United Nations treaty organization. The other two sectors of the ITU are Radiocommunication and Telecommunication Development. ITU-TS carries out the standardization role of the ITU. It is responsible for "studying technical, operating, and tariff questions and adopting recommendations on them with a view to standardizing telecommunications on a worldwide basis." ITU-TS assumes the standardization work of the former CCITT, together with some related work transferred from the CCIR. However, the former CCITT work aimed at aiding developing countries (e.g., the Special Autonomous Groups) will now be done in ITU's Telecommunication Development Sector.

The members of ITU-TS, because it is a sector of a treaty organization, are governments. Normally, the members of the ITU-TS are the national post, telephone, and telegraph (PTT) administrations.[7] ITU-TS is organized into 15 study groups (SGs). There are three areas of activity concerned with OSI matters: data communications, telematic services, and integrated services digital networks (ISDNs). Work in ITU-TS is focused on specific formal questions

---

5 The *ISO Technical Programme*, published in January and July, lists CDs, DISs, draft technical reports (DTRs), DADs, and DAMs in technical committee order. Each entry includes the target date, edition, title, and stage number.

6 At the 1992 Additional Plenipotentiary Conference in Geneva, major changes were made to the Constitution and Convention of the International Telecommunication Union (ITU). As a consequence, the work formerly done by the CCITT will be carried out in the Telecommunication Standardization (TS) sector of the ITU. The CCITT Secretariat has been replaced by the Telecommunication Standardization Bureau. The CCITT Plenary Assembly has been replaced by the World Telecommunication Standardization Conference (WTSC). The new Constitution and Convention will enter into force on 1 July 1994, however, the provisions relating to the new structure and working methods are applicable as from 1 March 1993. [Ref. SC21 N 7749 1993]

7 For example, the representation for the United States is from the Department of State.

posed at the beginning of the study period. In the three areas concerned with OSI matters, the work directly involves six SGs:[8]

- SG 1 on the operational aspects of telematic services
- SG 7 on data networks and open system communications
- SG 8 on terminal equipment recommendations for the telematic services
- SG 11 on switching and control signaling for telephony
- SG 13 on digital networks in general and ISDN in particular
- SG 14 on data transmission over the telephone network.

Within the ITU-TS, the Telecommunication Standardization Bureau replaces the CCITT Secretariat. The Telecommunication Standardization Advisory Group (TSAG), which will meet yearly has been established to:

- Review priorities and strategies
- Review progress in the implementation of the work program
- Provide guidelines for the work of study groups
- Recommend measures to foster cooperation and coordination with other standards bodies, with the Development and Radiocommunication Sectors, and with the Strategic Planning Unit in the General Secretariat.

Documents produced by ITU-TS are called recommendations, not standards; the term recommendation is used because ITU-TS does not have the authority of a standards body nor of its representative governments to prescribe implementation. Every 4 years, the ITU-TS holds a World Telecommunication Standardization Conference (WTSC) (formerly the CCITT Plenary Assembly) that establishes the work program for the next 4 years. This work program is composed of questions submitted by the SGs based on requests made by the various member organizations. The first WTSC (tenth CCITT Plenary) was held 1-12 March 1993 in Helsinki, Finland. The 1993-1996 work plan for ITU-TS Study Group (SG) 7 on Data Networks and Open System Communications, which has overall responsibility for technical collaborative work with ISO/IEC JTC1, is reproduced in Section 2 of Appendix G. Of particular interest to JTC1 are the following ITU-TS questions (a complete list of open and recently closed questions for JTC1/SC21 is provided in Appendix G):

- Q 5/7, Multicast
- Q 13/7, OSI Systems Management
- Q 14/7, Message Handling Systems
- Q 15/7, Directory Systems
- Q 16/7, Reference Model and Components for Open Distributed Processing
- Q 17/7, Testing of Data Communications Protocols
- Q 19/7, OSI Architecture
- Q 20/7, Security Services, Mechanisms, and Protocols for ITU-TS Applications
- Q 21/7, OSI Application Layer
- Q 22/7, OSI Presentation and Session Layers
- Q 23/7, OSI Transport and Network Layers
- Q 24/7, OSI Data Link and Physical Layers.

[8] Prior to 1993, roman numerals were used to identify study groups in CCITT.

At the end of the 4-year period, each study group prepares draft recommendations in answer to these questions and submits them to the new WTSC. If the WTSC approves these recommendations, the drafts are published as ITU-TS Recommendations. The most recent study period—1989 to 1992—ended in April 1992 and SG 7 endorsed 72 new or revised recommendations. In urgent situations (e.g., standardization of ISDN), the drafts can proceed through a special balloting procedure to become a ITU-TS Recommendation before the normal 4-year period has expired. The new series of recommendations, when published, supersedes the recommendations from all previous study periods. Previously, all recommendations produced in the same study period were bound in books of the same color. For example, the 1984 recommendations were known as the "Red Books" and the 1988 recommendations were known as the "Blue Books." ITU-TS has discontinued this practice [Ref. JTC1 N 1763 1992] and, as of 1989, each recommendation will be published as a separate brochure.[9] Wherever possible these are adopted as ISO standards.[10]

An information exchange system called TELEDOC is being developed in three phases by ITU headquarters for the exchange of information and documents between ITU-TS and its members. During the first phase, users will have access to:

- Circulars
- Collective letters
- Lists of contributions and delayed contributions
- Lists of study group reports
- Lists of ITU-TS recommendations
- Summaries of new or revised recommendations approved under ITU-TS Resolution No. 2
- ITU-TS meeting schedule and information concerning study groups.

At present, TELEDOC documents are available only in ASCII. Phases 2 and 3 are being developed and were expected to become operational in 1993. Members will then be able to access the text of ITU-TS recommendations. In addition, ITU plans to make available on CD-ROM the complete set of all recommendations by the end of 1993. [Ref. SC21 N 7490 1992]

A Guide for ITU-TS and ISO/IEC JTC1 Cooperation has been developed by the Collaborative Group on Procedures for ITU-TS and ISO/IEC JTC1 Cooperation. The most recent version is SC21 N 7747, April 1993.

---

9 Rapid progress in telecommunication technologies and services has led to a dramatic increase in the number and volume (since 1980, the volume has almost doubled every 4 years) of CCITT Recommendations, resulting in delays to produce the entire set every 4 years. CCITT concluded an unsuccessful experiment of electronically distributing their recommendations on the Internet in December 1991. Instead, it is now publishing each recommendation as a separate brochure and will publish a two-part *Catalogue of Recommendations*. Part 1 will consist of new and revised recommendations approved and published under the new system (updated and published every 6 months). Part 2 will be the complete and detailed list of all CCITT recommendations as currently published in the Blue Book. In May 1992, SC21 requested national body comment on whether the catalogue that CCITT is developing satisfies their requirements. [Ref. SC21 N 7132 1992]

10 Until recently, CCITT recommendations were available in the United States from Omnicom, Inc., 115 Park St. SE, Vienna, VA 22180-4607, 1-800-Omnicom. Phillips Publications in Potomac, Maryland, has taken over for Omnicom but uses the same phone number.

X/Open. X/Open consists of a staff of program managers and marketing managers and four groups of customers:

- X/Open Corporate members—system manufacturers who provide products and services of over $1 billion annually
- The System Vendor Council—system vendors who provide products and services of less than $1 billion
- The Independent Software Vendor Council—software vendors such as UNIX International (UI)/UNIX Systems Laboratories (USL)
- The User Council—users who represent large purchasers of these services.

X/Open funds a technical program based on the wishes of the Corporate Members since they provide the overwhelming majority of X/Open's operating budget. Specifications are sponsored by these manufacturers for inclusion in the X/Open suite of specifications. Some specifications are obtained in whole from other parties and "fast-tracked." In this case, the specification is sent to representatives of each Corporate Member and comments on the specifications are collected and "resolved." These companies then vote on whether the specification should become part of the X/Open specification. An example of a fast-tracked specification is the Phillips CD-ROM specification. Fast-tracked specifications may be offered by consortia in areas related to computer systems such as X.400 APIs, user interfaces, etc.

A specification that is not fast-tracked is referred to an X/Open working group for development. One of the most important working groups has been the Transaction Working Group. The working groups meet four to six times per year and attempt to adapt (or more rarely develop) a specification that is suitable. The "new specification" is studied by all of the X/Open Stakeholders, who then vote on acceptance. Again, a large fraction of the membership of the system manufacturers is required for acceptance.

Legal rights to distribute the specifications remain with X/Open. If these rights cannot be obtained, X/Open will not utilize its resources in promoting the specifications. X/Open "brands" products complying with its specifications. In order to determine compliance, X/Open has made significant investments in developing verification suites that ensure that an operating system and command sequence is compliant.

TSGCE. TSGCE develops and maintains technical standardization agreements (STANAGs) for NATO. TSGCE has a number of subgroups and project groups working on standards. For example, TSGCE SG9 has responsibility for the NATO OSI Reference Model and for developing OSI and ISDN STANAGs and profiles. Appendix F lists the various subgroups and project groups, and includes an organizational chart for NATO bodies in the fields of communication and information systems.[11] Chapter 18 provides an overview of the proposed reorganization of the TSGCE, and Chapters 17 and 18 describe the work of TSGCE in areas related to information systems.

Organizations Producing Standardized Profiles. Three international regional workshops of government and industry groups interested in implementation have been established to promote OSI and develop profiles. A Regional Workshop Coordinating Committee (RWCC) promotes dialog and harmonization among these workshops. The goal of the workshops is to define standards profiles that will ensure the interoperability of products from different vendors.

[11] NATO STANAGs are listed in *NATO Standardization Agreements and Allied Publications*, AAP-4 (1990), which is available (as are the STANAGs) from the NATO Subregistry at national MODs.

The European Workshop for Open Systems (EWOS) promulgates harmonized technical proposals for functional profiles of OSI standards and corresponding conformance test specifications. The Asia-Oceania Workshop (AOW) also prepares technical proposals for standardized profiles. The most active AOW participant is Japan. The OSE Implementor's Workshop (OIW) provides American-hemisphere input to the standardization of profiles. The workshop is hosted by NIST. The recommendations of this workshop form the basis for a multinational OSI specification, called Industry/Government Open Systems Specification (IGOSS), which will become the basis for the US and Canadian government open systems interconnection profile (GOSIP) (see Sections 16.1.3 and 16.1.7).

Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP). The US DoD DTMP manages technical activities within the DCPS area. It is concerned with the protocols required for information transfer on computer-to-computer networks. One of its primary missions is to manage and coordinate DoD representation to and coordination with US national, international, and commercial standards bodies for the purpose of influencing those bodies to incorporate military features in their base standards and profiles. It also develops coordinated DoD positions and recommendations, develops draft standards, prepares DCPS documents to support the acquisition process, and presents appropriate issues and products to the Standards Coordinating Committee (SCC) of the DISA Center for Standards (CFS).

The DTMP has the following fifteen approved standardization projects [Ref. Curcio 1994]:

- DoD Standardized Profiles for Message Handling Systems
- Network Management (NM) Standards for DoD Communications
- DoD DCPS Technical Reference Model
- Military Handbook 829 (MIL-HDBK-829)
- Validation Plan for Military Features in GOSIP Protocols and Architectures
- DoD Conformance/Interoperability Test Plan for Military Features in GOSIP Protocols and Architectures
- Multicasting Standards Development for OSI
- Defense Standardized Profile for Secondary Imagery System
- OSI Enhanced Communication Functions and Facilities (ECFF) for the Lower Layers
- Wireless Connectivity over Local Area Networks
- Security Labeling Options Protocol
- Incorporation of Secure Data Network Standards (SDNS) Protocols into OSI
- Interim Joint Task Force Data Communications Profile
- Development of a Security Standards Framework
- Influence ISO Generic Upper Layer Security (GULS) Development.

These projects are assigned to the following seven working groups in the DTMP [McLane 1992; Curcio 1994]:

- WG1, Lower Layers
- WG2, Upper Layers
- WG3, Security
- WG4, Network Management
- WG5, Architecture

- WG6, Registration (inactive as of October 1993)
- WG7, Testing.

2.4 Proposed Definitions for Terms Used in Information System Service Standardization

Table 1 provides the definitions of a number of technical terms used in this document and elsewhere in discussing information system and CCIS standardization. These definitions were derived from many sources and proposed by the US Corporate Information Management (CIM) Standards Office. [Ref. Keane 1991]

Table 1. Definitions of Terms for Information System Service Standardization

Application Software Interoperability: *The ability to have application software operating on heterogeneous* hardware/software platforms cooperate in performing some user function. (Source: NIST with modification)

Basic Interoperability: The exchange of data that preserves the meaning and relationship of the data exchanged. (Source: ATCCIS)

Buffer/gateway: Software or hardware used to compensate for a difference in rate of flow of data or time of occurrence of events or differences in protocol or in data representation when transferring data from one system to another. (Preliminary. Source: NATO Interoperability Management Plan (NIMP), Edition 2)

Compatibility: The capability of two or more items or components of equipment or materiel to exist or function in the same system or environment without mutual interference. [Source: Joint Chiefs of Staff (JCS) PUB 1]

Information system interoperability: The ability of systems to exchange data, in a timely manner, in support of a user-defined business decision process, and to preserve the meaning and relationships of the data exchanged. The degree of interoperability/information exchange (e.g., manual, limited automated, fully automated) is to be determined by the system users and developers.

Interoperability: The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. (JCS PUB 1)

Open Specifications: Public specifications that are maintained by an open, public consensus process to accommodate new technologies over time and that are consistent with international standards. (Source: IEEE POSIX 1003.0)

Open System: A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: to be ported with minimal change across a wide range of systems; to interoperate with other applications on local and remote systems; and to interact with users in a style that facilitates user portability. (Source: IEEE POSIX 1003.0)

Open System Environment (OSE): The comprehensive set of interfaces, services, and supporting formats, plus user aspects, for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles. (Source: ISO)

Portability: The ability to use application software and data on heterogeneous hardware/software platforms. (Source: NIST)

Scalability: The ability to use the same application software on many different classes of hardware/software platforms, from personal computers to supercomputers. (Source: NIST)

Taxonomy: A scheme for describing the orderly classification of objects according to their presumed natural relationship. The classification scheme is a system of signs and symbols (the vocabulary) that includes rules for the formation and transformation of admissible expressions (the grammar).

Technical Architecture: A set of standards such that information systems built to the standards are inherently interoperable. The degree of interoperability is to be specified by the functional user as part of the requirements definition process. (Preliminary. Source: Suggested by DMR and work in ATCCIS)

Source: *CIM Terminology*, Private communication from Mr. John Keane, US DoD CIM Standards Office, CIM/XI, 16 July 1991, UNCLASSIFIED.

2.5 Assessments of Standards

While many discussions on open systems focus on common operating systems (instead of standard interfaces) and portability, the primary concerns of CCIS users are: (1) interoperability across heterogeneous systems, (2) flexible architectures for organization-wide open systems computing, (3) heterogeneous networked database access, and (4) integrated open and proprietary

network management. Standards for interoperability therefore need to be selected to support areas such as network connectivity, data sharing, multi-client application support, and integrated systems management. [Ref. RNLA 1994, p. 22] These are the areas of services for which standards are described in this document.

There are a number of competing forces vying for control of the standards world. Users want everything standardized before they buy anything. Vendors want everything else standardized except the area in which they operate, so *their* products are not governed by standards, but all the products they depend upon are so governed. Areas that require more investment by users need more stability before being standardized. Rapidly changing technologies may never be standardized. Vendors that dominate a product area have no interest in open standards, and without their support, open standards have a very hard time catching on in the marketplace. Some areas demand international acceptance of standards and some do not.

The result of all this is a very delicate balance among openness, maturity, and timing. The standards community is grappling with this balance with the result that some of the standards processes are undergoing revision. ISO's dominance as the primary keeper of the seal of approval of international standards is being threatened. As noted above, ISO is searching for a faster route to consensus to maintain its role in the international arena. At the same time, X/Open is expanding its role as a link between consortia and the international community as a mechanism for gaining quicker acceptance of working standards in both worlds. And everyone is working hard to be a team player by maintaining liaison with everyone else. However, in areas where one vendor has established a position of architectural control, they are not giving it up, leaving users to wonder if standardization efforts in those areas will ever pay off.

Where possible, Chapters 4 to 14 provide assessments of the status of the standards in the 11 service areas. The main assessments appear at the ends of the chapters. Summary assessments, derived from the NIST Applications Portability Profile (APP) [Ref. NIST 1993], are provided in the beginning of most of the chapters in the form shown in Figure 5. Note, however, that such assessments change quickly as products emerge and gain widespread use.

	LOC	PAV	CMP	MAT	STB	DFU	PRL
Standard 1	○		○	●	○		
Standard 2	●	○	●	●	●	●	●
Standard 3			○		○		

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key:
● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: NIST, April 1993.

Figure 5. Example Summary Assessment

The notations of Figure 5 are defined as follows [Ref. NIST 1993]:

- Level of consensus. A low evaluation is given to specifications that are proprietary or are used by a very limited or specialized group of users, such as vendor consortia; a high evaluation is given for a specification that has already become a national or international standard; average evaluations are assigned for pubic domain specifications that are not standard, or that may be in the process of becoming a standard (i.e., standards committee work-in-progress), or that are widely available across various hardware/software platforms.

- Product Availability. A low evaluation is given to specifications for which only a very few proprietary products are available; high evaluations are given to specifications for which there is a wide variety of products available from various vendors across different application platforms; average evaluations are assigned to specifications that may be proprietary but have many products available from a variety of vendors, or that are public domain specifications with products readily available.
- Completeness. A specification is evaluated on the degree to which it defines and covers key features necessary in supporting a specific functional area or service. For example, a network security specification that includes all of the components described would be evaluated higher than others that do not include all of the features.
- Maturity. According to the underlying technology of a specification, a high evaluation indicates that it is well understood (e.g., a reference model is well-defined, appropriate concepts of the technology are in widespread use, the technology may have been in use for many years, a formal mathematical model is defined). A low evaluation indicates that it may be based on technology that has not been well defined and may be relatively new.
- Stability. A high evaluation means that the specification is very stable; no changes are expected within the next 2 years. A low evaluation indicates that significant or numerous changes are expected within a relatively short time (1 to 2 years), or that incompatibilities exist between current and expected releases of the specification. An average evaluation is given to those specifications that may have known changes forthcoming to replace features in the existing specifications.
- De facto usage. This evaluation criterion estimates the likelihood that a vendor will independently propose products that conform to this specification whether or not a reference specification is stated in the procurement documents. A high evaluation indicates that most proposed products will conform to the specification. A low evaluation indicates that it is unlikely that the vendor will propose products based on the specifications. An average evaluation indicates that vendors are just as likely to propose products based on the specifications as not (i.e., no clear determination exists). In the cases of low or average evaluations, it is imperative that users include a specification in procurement documentation. A low evaluation does not necessarily mean that products implemented on the specification do not exist. It can also mean that some vendors would rather provide products that are not based on the recommended specifications, such as proprietary implementations.
- Problems/limitations. Lower evaluations are assigned to specifications with severe restrictions on use or capabilities (e.g., licensing restrictions) or with known problems that tend to be too difficult or too numerous to overcome (e.g., new releases of the specification are not compatible with previous releases, or not enough is covered in the standard to be useful). An average evaluation is given to those specifications that require some minor additional facility in order to be fully effective in their intended environment. This additional facility may be provided by a related standard or other specification.

(This page intentionally left blank)

3. ARCHITECTURES, FRAMEWORKS, AND REFERENCE MODELS

This chapter describes high-level generic architectures, frameworks, and technology reference models.

3.1 Terminology

The terms architecture, framework, and reference model have been used in so many overlapping ways that the only way to know what they mean in a specific context is to ask the writer or speaker. Within this document, these terms have the following meanings:

Architecture The high-level structure of the systems in a specific group. The architecture should define all structural elements that are to be common to all the systems in the group, but that is not part of the definition.

Framework A software product that forms the basis of a more complete product, with the expectation that the remaining components will fit easily into the overall system. A software engineering environment (SEE) framework is an example of this type of framework. It may provide no functionality directly accessible to a user, but it is expected that the completed SEE will provide numerous tools that aid software developers. The notion of a framework implies that the framework product contributes in some way to the integration of the other components.[12]

Reference Model A specification for the structure of a technology suitable for identifying required standards for that technology. For example, the Basic Reference Model for Open System Interconnection defines the structure of networking technology as layers with a high-level definition of the function of each layer, but without defining the standards for either the service definitions or the protocols of any layer. The intent to serve as a structure for standards development is part of the definition of a reference model.

The US DoD has defined a high-level document to promote information system standardization, *DoD Technical Architecture Framework for Information Management (TAFIM)* [Ref. TAFIM 1993]. Under the definitions given above, this document is neither a framework nor an architecture, but it contains an architecture in Volume 2, *Technical Reference Model (TRM) and Standards Profile Summary*. Volume 3 addresses *Architecture Concepts and Design Guidance*. Volumes 1 (*Overview*) and 3 provide guidance outside the realm of standardization. Volume 4 is the *Implementation Manual*, and Volume 5 is the *Support Plan*. Volume 6 is a reference model called an architecture [the *DoD Goal Security Architecture* (*DGSA*)]. Volume 7 is *Information Technology Standards Guidance for an Open System Environment (ITSG-OSE)*. Volume 8 is the *DoD Human Computer Interface (HCI) Style Guide*.

Frameworks (as defined above) are not discussed further in this chapter. The only known efforts to develop standard frameworks are as the basis for an SEE. These are discussed in Chapter 4.

3.2 High-Level Generic Architectures

This section discusses the following high-level generic architectures: the ATCCIS architecture, the NATO C3 Architecture, the National Institute for Standards and Technology

[12] In ISO, a framework has more general meaning. Rather than a product, a framework in ISO is a specification that shows how various functions work and are related to other functions. Frameworks exist for security (ISO/IEC 10181) and management (ISO/IEC 10164).

(NIST) Applications Portability Profile (APP), the IEEE Portable Operating System Interface (POSIX) Guide, and the US DoD Technical Reference Model (TRM).

3.2.1 ATCCIS Architecture

The four ATCCIS facilities essential to basic interoperability—the exchange of data that preserves the meaning and relationships of the data exchanged—are the Data Management Facility (DMF), the Transfer Facility (TF), the Service Control Facility (SCF), and the System Management Facility (SMF). These four "Basic Facilities" provide the three mechanisms necessary for basic interoperability: providing end-to-end transfer of data; managing the storage, retrieval, and interpretation of data; and managing the first two mechanisms as the minimum capability to support basic interoperability. (An overview of the features of the ATCCIS architecture is given in Appendix A.)

The standards for CCISs addressed in this document are not limited to the Basic Facilities required for basic interoperability. Capabilities, such as portability of applications software, that support a more general concept of interoperability constitute *enhanced interoperability*. These are addressed in the ATCCIS architecture in such facilities as the Input/Output Facilities (IOFs) that provide interfaces to systems not conforming to the ATCCIS architecture; the Man-Machine Interface (MMI) Support Facility (MSF) that provides standard user interfaces, and Application-Level Facilities (ALFs) that provide common automated support for various command and control functions.

Five of the groups of services are essential to basic interoperability and thus to the four basic facilities of the ATCCIS architecture: data management (ATCCIS DMF), network services for OSI (ATCCIS TF), operating system interface services (ATCCIS SCF); and security services and system management services (ATCCIS SMF and other facilities). The other service areas will provide for enhanced interoperability: data interchange services and distributed computing (applicable to the DMF); user interfaces and internationalization (applicable to the MSF); graphics services (applicable to the MSF and ALFs); and software engineering services (applicable to ALFs)

3.2.2 NATO C3 Architecture

The NATO C3 Architecture is described in one part of the four-part *NATO Consultation, Command and Control (C3) Master Plan* [Ref. NACISC 1989]. Based on early work contained in the 1980-1982 Architecture Design Study (ADS), the ADS follow-on studies (STC Projects 85-3 and 86-1), and ATCCIS Working Papers (WP 11, WP 24, and WP 25), the NATO C3 Architecture applies to the NATO Command, Control and Information System (NCCIS), which comprises automated command and control information systems (ACCISs). Examples of NATO ACCISs are described in Chapter 18.

The NCCIS Architecture describes an automated CCIS in precisely the same terms used to describe ATCCIS: "a transaction processing system with a partitioned, partially replicated database, capable of supporting applications, and maintaining a consistent interpretation of the data across organizational boundaries" [Ref. NACISA 1989b]. As in ATCCIS, the NCCIS architecture employs the concept of basic interoperability to address: the need to communicate so as to permit the exchange of data, and the need to have a common interpretation of the data thus exchanged. The NCCIS Architecture identifies the following as required to achieve basic interoperability: international OSI information exchange standards, data dictionary, data model (defining logical structure of data), and database conceptual schema (logical database design).

The NCCIS Architecture uses the concept of enhanced interoperability to describe interoperability aspects that go beyond basic interoperability. In NCCIS, these apply only to NATO-owned systems for "higher degrees of interoperability to support other operational requirements, flexibility, and cost saving." Examples of areas where higher degrees of interoperability can be achieved in NCCIS are common and generic application programs and human-machine interface.

NCCIS identifies five major classes of services: information exchange, data management, system control, application support, and human-machine interface management. In NCCIS these services are discussed as functions. The standards identified for supporting the architectures are identical for NCCIS and ATCCIS.[13]

3.2.3 IEEE POSIX OSE Reference Model

IEEE P1003.0, *Draft Guide to the POSIX Open System Environment* [Ref. IEEE 1992], seeks to accelerate consensus on an open systems environment (OSE) for applications portability and provides guidance to users on how to develop applications profiles. Chapter 10 discusses the POSIX effort.

P1003.0 defines a POSIX OSE Reference Model that is the basis for the model shown in Figure 1 in Chapter 1. Both models use the same three high-level entities: Application Software Entity, Application Platform Entity, and External Environment. Some platform services are included in the application program interface (API) between the first two of these entities, and others are included in the external environment interface (EEI) between the last two of these entities. The models differ primarily in the groupings of platform services that make up the application platform entity. The POSIX OSE Reference Model identifies four classes of APIs (system, communications, information, and human/computer interaction), whereas the model adopted for WP 25 is more detailed, defining 11 classes: software engineering, user interface, data management, data interchange, graphics, network, operating system, security, system management, distributed computing, and internationalization.

3.2.4 NIST Applications Portability Profile (APP)

Section 15.1.3.3 discusses the APP developed by the NIST. The NIST approach to applications portability is based on an architectural approach that provides interfaces for functionality to accommodate a broad range of applications requirements. The functional components of the architecture are viewed as a "tool box" of standard elements that can be used to develop and maintain portable applications. These tools are based on an open systems concept and are required to be developed as an integrated collection of non-proprietary standards.

A full complement of standards should be available under the APP by 1995. [Ref. APP 1991] Version 2 of the *Application Portability Profile (APP): The U. S. Government's Open System Environment Profile OSE/1* was published in May 1993. It recommends standards and specifications, provides guidance in areas where standards do not exist for seven service areas, and makes strategic evaluations with respect to those standards. These seven service areas are: operating system, human/computer interface, data management, data interchange, software engineering, graphics, and network. Two additional services areas, called integral supporting

---

[13] The survey of standards adopted for the NATO C3 Architecture was primarily a set of excerpts from an early edition of WP 25.

services, are security and management. These service areas are all based on the high-level POSIX OSE Reference Model.

3.2.5 DoD Technical Reference Model (TRM)[14]

The US DoD has developed its Technical Reference Model (TRM) for Information Management to provide technical guidance for the acquisition, development, and support of DoD information systems and associated infrastructure systems. The TRM, shown in Figure 1 in Chapter 1, provides the high-level relationships of the domain showing the major service areas.[15] When populated with specific standards, the model defines a profile of technical standards that are *mandatory* for DoD information systems, except those that are specifically exempted by the US Information Technology Policy Board (ITPB). The model, while not a specific system architecture, defines standards and guidelines that can be tailored and applied to meet the needs of specific mission areas (i.e., mission or functional areas).

Figure 1 only depicts entities, interfaces, and service areas and does not imply relationships among the service areas. The Technical Reference Model adopts the foundation work of IEEE POSIX Working Group P1003.0 [*Draft Guide to the POSIX Open System Environment,* Draft 15, IEEE, June 1992]. The Technical Reference Model identifies services for the Application Platform Entity of the POSIX Open System Reference Model; identifies application program interfaces (APIs) such as system services, communications services, information services, and human-computer interaction services between the Application Platform Entity and the Application Software Entity; and external environment interfaces (EEIs) such as communications services, information services, and human-computer interaction services between the Application Platform Entity and the External Environment (at the bottom of the figure). The 11 service areas of the TRM match the eleven service areas treated in Chapters 4-14 of this document.

In April 1993, the Department of the Air Force, Electronic Systems Center (ESC), adopted a software standards policy based on the DoD Technical Reference Model. The ESC framework defines three sets of standards: one for embedded systems, one for command centers, and one for management information systems. [Ref. ESC 1993]

3.3 Technology Reference Models

The ISO and others have developed several technology reference models that are described in this document. These include:

- Open Systems Interconnection (OSI) Reference Model (ISO 7498) (see Section 9.1)
- Open Distributed Processing (ODP) Reference Model (CD 10746) (see Section 13.2)
- Office Document Architecture (ODA) Reference Model (see Section 7.1.1)
- DoD Goal Security Architecture (see Section 11.2.4.8)
- NIST User Interface Reference Model (see Sections 5.2.6 and 5.3)
- Object Management Group's (OMG) Object Management Architecture (see Section 13.3).

---

14 WP 25 was the survey of standards used to define the initial version of the TRM.

15 US DoD components are required to apply the TRM to increase commonality and interoperability across the Department, as directed by the Director of Defense Information (DDI) in February 1992 [Ref. DDI 1992].

4. SOFTWARE ENGINEERING SERVICE STANDARDS

This chapter identifies programming languages, software development environments, tool sets, process models, and methodologies, and other software engineering service standards. An overview of the status of key standards for software engineering services is given in Table 2.

4.1 Requirements for Software Engineering Services

Software engineering services address the sets of tools that support requirements definition, system development, testing, maintenance, and administration. They also address computer-aided software engineering (CASE), software development environments and tools, and library support.

In order to satisfy the overall requirement for using COTS/NDI hardware and software, software must be both portable and interoperable. Requirements for the efficient production of effective software dictate the use of software development environments and tools as well as reuse libraries. As the technology evolves, needs for expert system support in the software production process will arise.

4.2 Programming Languages

4.2.1 Ada Programming Language

Ada is a programming language agreed to be used within NATO and the US DoD[16] as a standard, general-purpose

Table 2. Status Overview of Key Software Engineering Service Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
Ada	●	●	●	●	○	○	○
C	●	●	●	●	●	●	●
COBOL	●	●	●	●	●	●	●
FORTRAN	●	●	●	●	●	●	●
PASCAL	●	○		●	●		
ECMA PCTE	●	○		○	○		

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: [Ref. APP 1993]

[16] DoD Directive 3405.1 states that Ada is the preferred computer programming language for all US DoD applications except when the use of another higher order language is most cost effective over the application's life cycle. DoD Directive 3405.2 mandates the use of Ada in all computers integral to weapons systems (embedded systems).

high-level programming language. It was introduced in 1979 after the US DoD became concerned about the proliferation of computer languages it was using and determined that none of these languages was suitable for writing DoD software. Ada uses the latest ideas in language design and a standard programming support environment is suggested. It was adopted in 1983 as a common standard by ANSI and US Military Standard (MIL-STD-1815A) and in November 1985 as a Federal Information Processing Standard (FIPS 119). In 1987, ISO endorsed it as an ISO standard (ISO 8652).

Ada 9X, the project to revise ANSI/MIL-STD-1815A has officially entered the ISO standardization process by being submitted for registration as a CD in September 1993. Balloting has begun. Ada 9X was also sent out for voting by ANSI, and DIS balloting is expected to begin in January 1994.

Proposed DoD policy regarding the transition to Ada 9X calls for a 2-year period after ISO approval when either Ada 83 or Ada 9X can be used. After this 2-year period, the use of Ada 9X will be required for new projects. As always, existing Ada 83 projects are free to baseline on Ada 83 compilers. In addition, to hasten the transition, prior to ISO approval the use of Ada 9X will be encouraged for research and development projects using a compiler in beta testing.

The Ada Semantic Interface Specification (ASIS) was developed to give tool developers access to the Ada syntactic and semantic information contained in Ada libraries. ASIS is an open standard that supports multiple CASE tools, multiple Ada compilation systems, and the ability to easily integrate proprietary tools. ASIS is an interface between the Ada library produced by a compiler for a program and any tool requiring information from that library.

4.2.1.1 Ada Programming Support Environment (APSE)

An APSE is an environment for developing software systems written in Ada. At its core is a kernel APSE (KAPSE), which represents general operating system services such as file management services and process and device control services, as well as object management services. It is at this level, as opposed to the outer layers, the MAPSE (Minimal APSE) and APSE, that a common set of interfaces is required. The MAPSE consists of software tools that minimally support software development, such as compilers, editors, and linkers, while the APSE provides project-specific tools and services. APSE is the subject of a special working group in TSGCE (see Section 17.3).

4.2.1.2 Common APSE Interface Set (CAIS)

CAIS provides a common set of interfaces to the KAPSE. The CAIS standard (US DoD MIL-STD-1838A, 1989) defines a set of interfaces that allows APSE tools to use common operating services and facilities in a standardized fashion. The original plan for the designing of CAIS in the United States called for one set of interfaces to be produced at the end of 4 years' work (the original target was 1987). As pressure mounted for an earlier release, the Ada Joint Program Office (AJPO) decided that a limited capability version should be provided before the full CAIS was complete.

The first version of CAIS (US DoD MIL-STD-1838) was published in October 1986. It was supposed to comprise only those interfaces common to two different APSEs being developed by the US Army and the US Air Force: the Ada Language System (ALS, for the Army) and the Ada Integrated Environment (AIE, for the Air Force). Because of divergent approaches at the KAPSE interface level taken by the ALS and AIE contractors, the KAPSE Interface Team (KIT)

and the KAPSE Interface Team from Industry and Academia (KITIA) were formed. Together, the KIT/KITIA produced the first version of the CAIS based on the entity-relation-attribute (ERA) model.

In parallel, the Requirements and Design Criteria Working Group (RACWG), composed of KIT and KITIA members, was established in July 1983 for the purpose of defining a set of requirements and criteria for the design of a second version of the CAIS. In 1985, a contract was awarded to SofTech, Inc., to continue development of this second version of CAIS (CAIS-A). CAIS-A was reviewed publicly in 1987 and was published as a military standard (MIL-STD-1838A) in April 1989 [Ref. AJPO 198?].

There are no plans, nor is a mechanism currently in place, to update CAIS-A. While there are three implementations of CAIS-A, the effort is generally suffering due to a lack of commercial support.

4.2.2 Pascal Programming Language

Pascal is a computer programming language originally designed to satisfy two principal aims: (1) to provide a language suitable for teaching programming as a systematic discipline based on certain fundamental concepts clearly and naturally reflected by the language and (2) to define a language whose implementations could be reliable and efficient on then-available computers. A Pascal standard was adopted in 1983 as ANSI X3.97 and IEEE 770.

At the same time that the ANSI/IEEE Pascal standard was being developed, the British Standards Institution (BSI) sponsored an ISO draft proposal for Pascal. In 1983, ISO adopted Pascal as a standard (ISO 7185), endorsing British Standard (BS) 6192-1982. While the ISO and ANSI/IEEE Pascal standards are compatible, there are some differences in technical substance as well as some errors in the ISO standard.

In January 1985 the US Federal Government adopted the ANSI/IEEE standard as FIPS 109. The implementation of FIPS Pascal involves three areas of consideration:

- Acquisition of Pascal processors
- Interpretation of FIPS Pascal
- Validation of Pascal processors.

On 10 April 1990, ANSI X3 and the IEEE approved the *Extended Programming Language Pascal* standard as IEEE 770 and ANSI X3.160. This was adopted in 1991 by ISO as ISO 10206.

4.2.3 C Programming Language

C originated in the late 1970s as the programming language of the UNIX[17] operating system. It is a general-purpose programming language that features economy of expression, modern flow control and data structures, and a rich set of operators.

C is not a very "high level" language, nor a complex one. Its particular area of application is systems programming (e.g., software for an operating system). Although it was originally implemented on a DEC PDP-11, it is now widely used. [Ref. Kernighan 1988]

Its growing popularity, changes in the language over the years, and the creation of compilers by groups not involved in its design raised the need for a standard in the early 1980s.

[17] UNIX is a registered trademark of Unix System Laboratories, a wholly owned subsidiary of Novell, Inc.

[Ref. Kernighan 1988] In 1989, ANSI promulgated X3.159, *Programming Language C.* In 1990, this standard was adopted by ISO (ISO 9899). It was also recently approved by the US Federal Government as FIPS-160.

There is an ASC X3 project (0743-D) to promulgate a standard for Programming Language C++, a higher-level update of C. There is no draft standard yet, but estimated completion is 1994. According to a recent study by UNIX tool supplier Lucid [Ref. OSN 1993j], businesses are moving from C to C++ faster than expected with 80 percent of the market either using or in transition to C++.

Technical Committee ANSI X3J11 of ASC X3 is developing a technical report (TR) for numerical C extensions. The objective of the report is to outline the technical issues involved in adding more support for numerical programming in Programming Language C. The issues that have been identified are [Ref. X3 1991h]:

- Optimization of potentially aliased variables
- Support for vector hardware
- Complex arithmetic
- Variability dimensioned arrays
- IEEE issues including infinity
- Exception handling
- Support for parallel processing
- Syntax for array/matrix operations.

To date, three subgroups have completed their work, resulting in the publication of Parts 1-3 of the report for comment. The parts are:

- Part 1: *Designated Initializers and Compound Literals*
- Part 2: *Aliasing Control via Restricted Pointers*
- Part 3: *Floating-Point C Extensions.*

ANSI X3 recently announced the approval of a new project for Programming Language C Information Bulletins under the auspices of ANSI X3J11. ANSI X3J11 has compiled numerous requests for interpretation or clarification of ANSI X3.159-1989, and the bulletin will provide a means of making those interpretations available to the public. [Ref. X3 1991m]

4.2.4 COBOL Programming Language

COBOL programming language, which is primarily used for business applications, is an ANSI (X3.23-1985) standard that was also adopted in 1985 by ISO (ISO 1989). It was adopted by the United States in 1986 as FIPS 21-2. ISO 1989 has one amendment, *Intrinsic Function Module*, 1992.

ANSI X3J4 is developing a revision of standard COBOL that is scheduled to be available for public review in 1995 or 1996. This revision will be an upward compatible enhancement of two existing COBOL standards:

- X3.23-1985[R1991], *Programming Language COBOL*
- X3.23a-1989[R1991], *Intrinsic Function Module for COBOL* (ISO 1989 AM 1).

Other work undertaken by X3J4 includes interpretation of the existing COBOL standard and development of three addenda: (1) *Correction of Errors and Resolution of Ambiguities*, (2) *Support for Multi-Octet Character Sets*, and (3) a native language binding for the Forms

Interface Management System (FIMS) being standardized (see Section 5.2.9) by the Conference on Data Systems Languages (CODASYL) FIMS Committee. [Ref. X3 1992g]

In October 1992, ANSI X3 announced the formation of a new task group, X3J4.1, object-oriented COBOL. The task group will be responsible for producing a technical report for the purpose of submitting potential object-oriented extensions for review and comment before they are incorporated into the next revision of COBOL standard X3.23-1985. X3J4.1 will continue the work of the object-oriented COBOL Task Group formed in 1989 by the CODASYL COBOL Committee. [Ref. X3 1992i] The current standard does not include real-time, operating system, or communications components, although this may change with the functionality introduced by proposed revisions [Ref. APP 1992].

4.2.5 FORTRAN Programming Language

In 1978, ANSI promulgated a standard for FORTRAN (ANSI X3.9), a programming language for scientific numerical computation that has wide use and many variations. In 1980, this standard was endorsed by ISO (ISO 1539) and is now in Edition 2 (ISO 1539:1991). FIPS 69 adopted X3.9-1978 in September 1980 as a US standard to promote portability of FORTRAN programs for use on a variety of data processing systems. The most recent FIPS (FIPS 69-1) was issued in December 1985; a revised ANSI standard was issued in 1989. An ANSI X3J3 project X3.198 produced an extended version of FORTRAN (*Programming Language FORTRAN 90*) in 1992. Non-standard versions of FORTRAN exist, posing potential interoperability problems.

4.2.6 LISP and Prolog Programming Languages

LISP is currently the most popular computer language used in artificial intelligence (AI) programming in the United States, although Prolog standardization efforts are underway in the United Kingdom. LISP is designed for supporting symbolic manipulation and the interactive, trial-and-error style of programming employed by many AI researchers. It was invented in 1958 and has many dialects. The dialects tend to fall into two main camps: INTERLISP and MACLISP. In the interest of standardization, Common LISP was developed. [Ref. Steele 1984] It is not yet an official standard, but was created at the initiative of many vendors and is increasingly becoming the preferred version. Common LISP compilers exist for several mainframe computers [Ref. Schutzer 1987], minicomputers, and microcomputers. The Standards Committee ANSI X3J13 is working on an ANSI standard for Common LISP (X3.226, *Programming Language Common LISP*, draft).

Except for efforts to standardize Scheme (IEEE 1178, which was approved in December 1990) and the AI programming language Prolog, there are currently no other standards for knowledge-based specifications or notations. (Knowledge-based systems are discussed in Section 4.3.3, and knowledge engineering is discussed with distributed system services in Section 13.5.3.)

4.2.7 BASIC Programming Language

BASIC is distinguished from other programming languages in its concern for the unsophisticated or novice user. While BASIC is a general-purpose programming language, it is designed primarily to be easy to learn, easy to use, and easy to remember. It is oriented toward, but not restricted to, interactive use. Its constructions are kept simple and special rules are kept to a minimum. The ANSI standard for Minimal BASIC (X3.60) was promulgated by ANSI in 1978 and adopted as FIPS 68 in 1980. It was subsequently adopted by ISO in 1984 (ISO 6373). In

1987, ANSI withdrew X3.60-1978 and superseded it with a standard for Full BASIC (X3.113-1987), which was adopted as FIPS 68-2 in August 1987 and by ISO in 1991 (ISO 10279). This revision reflects major changes, improvements, and additions to the BASIC specification. In December 1989 ANSI issued the standard ANSI X3.113A, *Addendum to Programming Language Full BASIC, Modules, and Individual Character Input.*

4.2.8 Fourth Generation Languages (4GLs)

Historically, there have not been any standards for fourth generation languages. One effort to address this deficiency is the work of ANSI X3J19, Xbase. Xbase is an application development language derived from Jet Propulsion Data Management and Information Center, a mainframe-based package. The first broadly successful product based on Xbase was dBase II in 1981. Currently available products using the Xbase language include dBase IV, dBase III Plus, Fox Base Plus, Fox Pro, dBFast, Clipper, Arago Quicksilver, Arago dBXL, Force Recital, Vulcan, and qBase. Xbase products are currently available for DOS, UNIX, Windows,[18] OS/2, VMS, Ultrix, and Solaris. [Ref. X3 1992e] The basic standard was expected to be on the street for worldwide coordination by the fall of 1993.

4.3 Standards for Software Environments

4.3.1 Bindings

In addition to programming language standards, several standards provide interfaces or connectivity between programming languages and applications. Such "bindings" exist or are being proposed for such standards as POSIX (IEEE P1003), *Graphical Kernel System* (GKS, ISO 7942), three-dimensional GKS (GKS-3D, ISO 8805), *Programmer's Hierarchical Interactive Graphics System* (PHIGS, ISO 9592 and 9593), *Information Resource Dictionary System* (IRDS, 10728), and *Computer Graphics Interface* (CGI, ISO 9636 and 9638).

POSIX bindings are now being developed only for Ada and FORTRAN. IEEE 1003.5, *Ada Bindings for POSIX,* and IEEE 1003.9, *FORTRAN Bindings for POSIX,* were approved in June 1992. IEEE work on a C binding for POSIX and FORTRAN 90 language bindings has been withdrawn. Work on Ada real-time bindings is now in P1003.5b (formerly P1003.20).

ANSI and ISO have approved standards for FORTRAN, Pascal, Ada, and C bindings for GKS. They are:

- ISO 8651-1 (Part 1): *FORTRAN Binding* (ANSI X3.124.1-1985), 1988
- ISO 8651-2 (Part 2): *Pascal Binding* (ANSI X3.124.2-1985), 1988
- ISO 8651-3 (Part 3): *Ada Binding* (ANSI X3.124.3-1985), 1988
- ISO/IEC 8651-4 (Part 4): *C Binding* (ANSI X3.124.4-1991), 1991.

ISO standards are being developed for GKS-3D bindings for FORTRAN and Ada. The C binding has reached IS status. Pascal and LISP bindings are under development. They are:

- DIS 8806-1 (Part 1): *FORTRAN Binding*, 1988
- DIS 8806-3 (Part 3): *Ada Binding*, 1989
- ISO/IEC 8806-4 (Part 4): *C Binding*, 1991

[18] X-Window System (commonly referenced as X-Windows) is a trademark of the Massachusetts Institute of Technology. Windows is a registered trademark of Microsoft Corporation.

- *Pascal Binding* [SC24 N 190] (ANSI Project 0545-I)
- *LISP Binding* (ANSI Project X3.122.5-199x).

There are ISO standards for Ada, FORTRAN, and C bindings to PHIGS. The Pascal binding is awaiting balloting. The standards are:

- ISO/IEC 9593-1 (Part 1): *FORTRAN Binding* (ANSI X3.144.1-199x), 1990
- DIS 9593-2 (Part 2): *Pascal Binding* (ANSI X3.144.2-199x)
- ISO/IEC 9593-3 (Part 3): *Ada Binding* (ANSI X3.144.3-199x), 1990
- ISO/IEC 9593-4 (Part 4): *C Binding* (ANSI X3.144.4-1992), 1992.

The FORTRAN, Pascal, Ada and C bindings to CGI are:

- ISO 9636, *Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification*
  - WD 9636-8 (Part 8): *FORTRAN Language Binding of CGI*, 1989
  - WD 9636-11 (Part 11): *C Language Binding of CGI*, 1989
- ISO 9638, *CGI Interface Techniques for Dialogues with Graphical Devices - CGI Language Bindings*
  - DIS 9638-1 (Part 1): *FORTRAN*
  - DIS 9638-2 (Part 2): *Pascal*
  - DIS 9638-3 (Part 3): *Ada*
  - DIS 9638-4 (Part 4): *C.*

IRDS bindings are as follows:

- ISO 10728/PDAM 1, *C Language Binding*, 1993
- ISO 10728/WDAM 2, *Ada Language Binding*, 1993.

Specification for a Set of Common Language-Independent Data Types (CLID) [ISO 11404] defines specific common language-independent data types by the following [Ref. X3 1991n]:

- Identifying distinct data types by their characteristics, functions, values, value-relationships, etc.
- Assigning identifiers, or formal reference syntax, to each distinguished data type
- Defining a means by which users or related standards may define additional data types
- Defining the form of and requirements for mappings between the data types of a programming or specification language and the language-independent data types defined by the standard.

ISO/IEC JTC1/SC22/WG11 on Binding Techniques for Languages has several projects underway, some of which are broader in scope than the name of the WG suggests. The following work items have been assigned to SC22/WG11 [Ref. SC21 N 5682 1991]:

- DTR 10182, *Binding Techniques for Programming Languages*, February 1992. The scope of this technical report is to classify language binding methods, report on particular instances in detail, and produce suggested guidelines for future language binding standards.
- *Specification for a Model for Common Language-Independent Procedure Calling Mechanisms (CLIPCM or CLIP)* [SC22/WG22 N 194R]. This project intends to specify a generic way for referencing procedures. A draft was circulated among SC22 member bodies for registration as a CD document in February 1991.
- CD 10967-1, *Language Compatible Arithmetic - Part 1: Integer and Floating Point Arithmetic*. The focus of this standard is on the portability of single language

programs across diverse platforms. Part 2 will deal with complex arithmetic and mathematical procedures. [Ref. X3 1992k]

Bindings for fourth generation languages (4GLs), however, have yet to be standardized. This could pose a problem if 4GLs were used for database queries.

Other Ada binding standards include the following:

- Generic Package of Elementary Functions (GPEF)—currently being formatted as a draft international standard. Ada, unlike other languages, does not include built-in or predefined elementary functions such as SQRT, SIN, and EXP. The proposed standard will specify 20 mathematical functions.
- Generic Package of Primitive Functions (GPPF)—accepted for voting by Numerics Rapporteur Group. It is intended to provide primitive operation required to endow mathematical software, such as implementations of the elementary functions, with the qualities of accuracy, efficiency, and portability. The package contains primitive functions and procedures for manipulating the fraction part and the exponent part of machine numbers of the generic floating-point type. Additional functions are provided for directed rounding to a nearby integer, for computing an exact remainder, for transferring the sign from one floating point machine number to another, and for shortening a floating point machine number to a specified number of leading radix digits.

Bindings for the following are described elsewhere in this document: SQL (Section 6.2.2.2); Transmission Control Protocol (TCP)/Internet Protocol (IP), (Section 9.7.4); X-Windows (Section 5.2.5), Motif[19] (Section 5.2.7), and OPEN LOOK[20] (Section 5.2.8).

4.3.2 Software Engineering Environments (SEE)

A *software engineering environment* consists of a set of tools cooperating harmoniously together to support specific processes through interoperability, sharing of data (via a uniform data repository), and presentation style. [Ref. Yeh 1992] Five SEE specifications are discussed in the paragraphs below: NIST/ECMA Reference Model, Portable Common Tool Environment (PCTE), integrated computer-aided software engineering (ICASE), Manufacturing Automation Programming Language Architecture (MAPLE), and Next Generation Computer Resources (NGCR).

4.3.2.1 NIST/ECMA Reference Model

ECMA and NIST have jointly produced a *Reference Model for Frameworks on Computer Assisted Software Engineering Environments*, Third Edition, August 1993 (ECMA Technical Report 55; NIST SP 500-211). ECMA TC33 Technical Group on Reference Models (TGRM) initially developed the framework, which the NIST Integrated Software Engineering Environment (ISEE) Working Group adopted, enhanced, and extended to support NIST goals. The NIST/ECMA Frameworks Reference Model defines many services, grouping them into object management, process management, communication, operating system, user interface, policy enforcement, and framework administration.

NIST is also working to establish a Federation of Integrated SEE Laboratories (FEDISEE). FEDISEE goals would be (1) to act as a technology exploitation and transfer mechanism for distributed computing and distributed repositories and (2) to develop a distributed development

---

[19] OSF/Motif is a trademark of the Open Software Foundation, Inc.

[20] OPEN LOOK is a trademark of Unix System Laboratories, a wholly owned subsidiary of Novell, Inc.

environment. The NIST ISEE Laboratory would serve as the focal and coordination point. The Federated environment would be a coalition of distinct, individual software engineering environments that can function together or independently. Users will have the perspective of a single system image of a distributed environment and repository. [Ref. Martin 1992] (Distributed computing is discussed in Chapter 13.)

4.3.2.2 Portable Common Tool Environment (PCTE)

Another software engineering environment standardization project is the PCTE (DIS 13719). Other projects standardize the interfaces between tools that might be combined to create an environment. Of particular interest are CASE tools (see Section 4.3.2.3 below).

PCTE Development and Standards. The PCTE project was begun in 1983 by the Commission of the European Communities (CEC) European Strategic Programme for Research in Information Technology (ESPRIT). ECMA Technical Committee 33 developed and standardized the *ECMA PCTE Abstract Specification* (ECMA-149) in December 1990. [Ref. Davis 1990] The C *Programming Language Binding to PCTE* (ECMA-158) was approved in June 1991. An Ada *Programming Language Binding* (ECMA-162) was completed in December 1991. A C++ binding is expected in June 1994. [Ref. Davis 1992] Second editions of the Basic ECMA Standards for PCTE (ECMA-149, ECMA-159, and ECMA-162) are ready to be submitted for ISO standardization. At its plenary in June 1993, SC21 resolved to propose PCTE as a fast track DIS (DIS 13719). [Ref. SC21 N 8081 1993] DIS 13719 is a three-part standard that includes ECMA-149, ECMA-158, and ECMA 162.

The goal of the PCTE project was to describe and prototype tool interfaces that could be used to define a software development environment. The environment would comprise a set of *public tool interfaces (PTIs) as well as a data management system.* As defined by the PCTE project, a PTI is a non-proprietary interface existing as a library unit that may be used by a tool to provide access to system services. Tool builders might use the interfaces to either integrate or attach their tool products to an environment. The distinction between integration and attachment reflects the degree to which the environment monitors, controls, and makes use of the information on a given tool. An integrated tool makes full use of the services provided by the environment, such as logging an audit trail and data management. An attached tool does not; for example, data are maintained in a repository known only to that tool.

The criteria for development of the PCTE were that it be policy and mechanism independent, support a distributed environment, provide easy tool integration, provide a complete interface definition, and provide multi-language support. To accomplish this, PCTE defines the services needed by the tools. The services provided by PCTE include data management, tool execution and communication, distribution and environment management, and programmer interface for user interface management.

Convergence with CAIS-A. The Portable Common Tools Interface Set (PCIS) project was created to resolve the unsatisfactory situation that had arisen in the late 1980s, that the independent efforts of Europe and the United States to produce a PTI had resulted in two contenders for an international standard, PCTE and CAIS-A (see Section 4.2.1.2). In an attempt to discover a convergence path, a study was carried out in 1988 and 1989, jointly on behalf of the Independent European Programming Group Technical Area 13 (IEPG-TA13) and the AJPO. This study concluded that it would be feasible to make a union of the two PTIs and in August 1989 the AJPO and IEPG agreed to pursue the convergence path. The name "PCIS" was coined by

appropriately "converging " the acronyms PCTE and CAIS-A. PCIS later agreed, however, to abandon the path of convergence and has based its framework definition upon PCTE, virtually to the exclusion of CAIS-A. PCIS may therefore be regarded as a set of proposals for enhancements to PCTE. [Ref. Boyer 1993]

Organizations Promoting PCTE. The PCTE Interface Management Board (PIMB) Association (see Appendix F) is a non-profit international company whose purpose is to promote greater use of the PCTE interface and to encourage development of tools and software engineering methodologies using PCTE. [Ref. Vernocchi 1992]

The North American PCTE Initiative (NAPI) was formed in October 1992 by the US DoD, NIST, and Object Management Group to increase the visibility and use of PCTE and to accelerate the evolution of PCTE and its adoption as a standard. [Ref. Davis 1992] The first NAPI meeting was held November 1992 at NIST. [Ref. NAPI 1992]

Relation of PCTE and IRDS. Noting a major overlap between PCTE and ISO 10728, *IRDS Services Interface,* SC21 is recommending the following fast-track procedure [Ref. SC21 N 8103 Revised 1993]:

- Circulate the PCTE document for review by JTC1 national bodies
- Call a joint meeting of the concerned subcommittees with ECMA to allow discussion of appropriate action in relation to the overlap.

One option to address the overlap is to incorporate those PCTE functionalities not in ISO 10728 into future IRDS versions [EWOS 1991a]. One comment from a PCTE supplier (EDS SCICON) noted that PCTE provides a rich set of security facilities, mandatory and discretionary, that have nc parallel in IRDS, making IRDS unsuitable (in their view) for safety-critical systems or secure systems.

In December 1993, the UK Government Centre for Information Systems, Central Computer and Telecommunications Agency (CCTA) completed a thorough review of this overlap. This comparison noted the following differences [Ref. DISC 1993b]:

- Services in ISO 10728 for which there are no PCTE equivalents:
  - Information Resource Domain (IRD) creation and removal (the equivalent functionality is outside the scope of the PCTE DIS)
  - Open and Close IRDS (the equivalent functionality is outside the scope of the PCTE DIS)
  - Creation and manipulation of reference paths between working sets
  - Two-phase commit
  - Get Diagnostics, which provides detailed information about an error code
  - Open Cursor (specifying a query expression), Retrieve Object using a cursor, and Close Cursor
  - Declassify Object (PCTE provides an equivalent to Reclassify, to make an object more tightly typed, but not the converse)
  - Change of Working Set Content Status to uncontrolled (updateable), controlled (frozen), or archived.
- Facilities found in the new extensions to IRDS for which there are no equivalents in ISO 10728 or in PCTE:
  - Registration of operations, methods (in an object-oriented programming sense), and their parameters
  - Invocation of operations.

- PCTE services not provided by ISO 10728 or its extensions:
  - Process Management Services, including pipes, files, a notification service, and message queues
  - Nested commit and rollback, which allows a controlling activity to abort the work of one of its subactivities even after the subactivity has gone "commit"
  - Maintenance of replicas of objects on replica volumes
  - Operations to connect workstations to the PCTE installation and later disconnect them, along with miscellaneous file copy and time functions.

The report noted that it would be possible to provide a PCTE object management set of services implemented on top of the ISO IRDS Services Interface and that it would be possible to do the reverse as well. However, the report suggested it would be more likely that implementors will provide both interfaces to the same underlying database. Suggestions included in the report could serve to improve the compatibility between the standards, making the two object management systems more similar and hence easier for a vendor to provide both interfaces to the same underlying repository. Additional comments contained in the report including the following [Ref. CCTA 1993]:

- Improving compatibility might be the best way forward for the user community, who would like their CASE tools to interoperate, whatever standard the CASE tool vendor chooses to use. A greater degree of compatibility would make it easier for vendors to offer one product, storing its information in one database, and supporting both interfaces.
- It is likely that large sites will end up not only with both IRDS and PCTE products but also with products using other, de facto repository standards and with products using proprietary repositories. Interoperability will become a major issue for such sites. It may therefore be important for both IRDS and PCTE developers to work in wider communities on the general problem of interoperability, for example, on common object models and abstract schemas that can be mapped to both IRDS content modules and PCTE Schema Definition Sets.

4.3.2.3 ICASE

IEEE 1209, *Recommended Practice for Evaluating CASE Tools* was approved in 1992. The Institution of Electrical Engineers (IEE)/British Computer Society Joint Working Party on Software Engineering Standards has also discussed the possibility of investigating CASE tools and, in particular, the way in which their use supports conformance to high quality standards. However, the only planned activity was to comment on IEEE P1209. In discussions related to a proposed UK MOD standard (DEF-STAN-00-55), *Requirements for the Procurement of Safety Critical Software*, the remark has been made that currently available CASE tools would not meet their requirements, since none of the tools has been or can be subject to the kind of formal methods analysis laid down in the proposal [Ref. Kemp 1990].

Another issue with respect to tools and toolsets is the ability to interconnect tools from different software developers. Consequently, the IEEE Computer Society approved a project authorization request (PAR) for a *Standard Reference Model for Computing System Engineering Tool Interconnections* (P1175) in February 1988. The core of this standard is the Standard Text Language (STL), which describes concepts such as data, conditions, events, and states, as well as transformation, control-transition, and state-transition operations. The standard supports both textual and graphical forms. [Ref. P1175 1989] It was approved in 1991 and a PAR for its

revision was approved October 1993. ANSI X3H6 on CASE Tool Integration Models (CTIM) was recently formed.

The CASE Integration Services (CIS) Committee is also trying to provide direction for integration standards in the CASE arena. Originally formed to discuss a standard interface for services to assist in the integration of software engineering tools into CASE environments, the CIS committee is now a public forum with many organizations participating in its deliberations and others monitoring the process as observers. The CIS committee has chosen to focus on two areas: (1) data integration, the sharing of meta-data among tools, and, (2) control integration, the sharing of control information among tools.

A standard known as ATIS (Atherton Tools Integration Services, or alternatively, A Tools Integration Standard) [Ref. CIS 1990], which was developed jointly by Digital Equipment Corporation and Atherton Technology, was proposed as a Base Document for the CIS work and is under review by committee members. ATIS is based on the object-oriented interfaces in Atherton Technology's Software BackPlane product. While it addresses many of the integration issues, it does so as a monolithic solution and has several deficiencies. However, the general solution offered by ATIS, (i.e., an object-oriented approach based on defined and extensible schema and methods) is considered by CIS members to be the preferred approach to providing integration services. Thus ATIS can provide a starting point for the ongoing work of CIS. [Ref. Nolan 1990] At CIS's request, ANSI is considering making CIS a group to pursue this standards issue.

Another standardization activity in this area is the CASE Data Interchange Format (CDIF) effort. The CDIF Technical Committee operates under the authority of the Electronic Industries Association (EIA), and its charter is "to develop an ANSI standard (eventually to become an ISO standard) for the exchange of information between CASEs." Three releases of standards are planned: a framework standard, a syntax standard, and a semantic standard. Their EIA Project Numbers (PNs) are 2387, 2389, and 2329, respectively. [Ref. Ornstern 1991] These standards are currently in interim form with plans to re-issue them early in 1994. [Ref. Boyer 1993] Both Continuous Acquisition and Life Cycle Support (CALS, formerly Computer Acquisition and Logistics Support) and P1175 representatives have participated in the meetings.

ANSI X3 has begun a development project for IRDS *Extensions to Support CASE Environment for Information Interchange*. This standard would define an IRDS, based on ANSI X3.138-1988, capable of supporting the full range of IRDS applications. In particular, it would be capable of acting as the IRD in a traditional data processing environment and capable of providing the stable store necessary to support an ICASE environment. The standard would include both the semantics of the IRDS and a software interface suitable to the needs of active CASE and Dictionary tools. The development has been assigned to Technical Committee ANSI X3H4.2. [Ref. X3 1990]

4.3.2.4 MAPLE

Work on a programming language environment architecture by ISO TC194/SC5 has resulted in ISO/TR 1286, *Manufacturing Automation Programming Language Environment Architecture (MAPLE)*, 1993. The project specifies the components of MAPLE (services and libraries), the interrelation between these components and the development of functional specifications for the components. It does not cover the implementation of the components. Adherence to the architecture is expected to reduce programming time, increase program quality, and reduce cost of integration. [Ref. SC21/WG3 N 1371 1992]

4.3.2.5 NGCR

Another environment reference model project is the US Navy Next Generation Computer Resources (NGCR) Project. The program revolves around the selection of interface standards in six areas. The interface standards will be based on existing industry standards with multi-vendor support. The objective is to restructure the Navy's approach to take better advantage of commercial advances and to reduce cost and duplication of computer resources. One of the areas chosen by NGCR for interface standardization is that of project support environments (PSEs). The initial focus for the PSE Standards Working Group (PSESWG) is to identify areas in support environments that are in need of standardization and for which industry accepted standards may be available within the NGCR's time frame. The primary goal of the PSESWG is to provide an interface standard that can be used by project managers as an aid in procuring or assembling a PSE. The first step towards this goal is the establishment of a reference model. The approach taken in the NGCR reference model is most directly comparable to the approach evidenced in the POSIX OSE and the NIST/ECMA Reference Model. The intent of the NGCR Reference Model is to encompass the domain of both the OSE and NIST/ECMA domains. The approach is explicitly aimed at establishing a conceptual basis for an environment, not at standardizing any particular environment product. [Ref. NGCR 1993]

4.3.3 Knowledge-Based Systems (KBSs)

Areas where standards are lacking, probably due to technological immaturity, include knowledge-based systems (KBSs) and software repositories. There are no standards for knowledge exchange, knowledge management, or development of knowledge bases for life-cycle maintainability. Several standards exist or are under development in the areas of software process models and development methods.

The UK General Expert System Methods Initiative (GEMINI) is an example of a project that is addressing needs for knowledge-based standards. In mid-1988, the CCTA launched this project to lay the foundation for a systematic KBS development methodology. A feasibility study concluded that there is strong support for such a method and that its development is both timely and feasible. [Ref. Montgomery 1989]

On March 1991, the IEEE Standards Board approved a PAR for the development of a *Standard for an Architecture for Knowledge Representation*. The IEEE Project number is P1252. [Ref. P1252 1991] This project is expected to address issues broader than KBS, development methods, and tools.

An important method of integrating KBSs is by means of the IRDS (ISO 10027). The first area of standardization for expert systems will likely be bindings between expert systems and programming languages, databases, and user interfaces. Progress towards providing decision support and decision making tools and methods is slow but may be stimulated by the early release of the IBM Repository. [Ref. MODITSB 1989]

4.3.4 Software Repositories and Reuse

Software repository standards to facilitate software reuse do not yet exist. These might include library structure, cataloging scheme, retrieval, documentation and maintenance, validation and verification, and reuse policy and guidance standards. Reuse is a strategy with potential to increase software productivity, reliability, and quality. A 1993 report published by Ovum finds that while repositories and frameworks promise many benefits for systems engineers, products

available at present are poor. Nearly all need to become less proprietary, use more off-the-shelf tools, and be enhanced to offer wider functionality. [Ref. OSN 1993k]

4.3.5 Process Models and Development Methods

A model of the software development process is the ordered sequence of activities that occur during the course of software development. Examples of software development process models include the waterfall model, rapid prototyping, and the spiral model. By contrast, a software development method (methodology) is the way the specific development activities are actually carried out by the developer. An example is the object-oriented method.

There is currently a single US standard, DoD-STD-2167A, *Defense Software Development Standard*, for the process of software development. It supersedes DoD-STD-2167, which was tied to the waterfall model and did not easily allow tailoring to other models. ANSI and the American Institute for Aeronautics and Astronautics (AIAA) recently issued a related standard, *Guide for Implementing Software Development Files Conforming to DoD-STD-2167A* (ANSI/AIAA G-009-1991).

The DoD is revising DoD-STD-2167A and harmonizing it with DoD-STD-7935A to develop a new standard called MIL-STD-498 (*Software Development and Documentation Standard*). Over 30 issues are being addressed during this harmonization effort, one of which is the compatibility of DoD-STD-2167A with the Ada programming language. [Ref. Singh 1992]

The IEEE publishes a volume of Software Engineering Standards [Ref. IEEE 1983] comprising 17 standards developed for software engineering. Most of the standards are joint ANSI/IEEE standards, and they provide recommendations reflecting the state of the art in the application of engineering principles to the development and maintenance of software. The 17 standards are the following (these and other ANSI/IEEE standards are listed in Appendix H):

1. ANSI/IEEE Std. 610.12 - *IEEE Standard Glossary of Software Engineering Terminology*, 1990
2. ANSI/IEEE Std. 730 - *IEEE Standard for Software Quality Assurance Plans*, 1989
3. ANSI/IEEE Std. 828 - *IEEE Standard for Software Configuration Management Plans*, 1990
4. ANSI/IEEE Std. 829 - *IEEE Standard for Software Test Documentation*, 1983
5. ANSI/IEEE Std. 830 - *IEEE Guide for Software Requirements Specifications*, 1984
6. IEEE Std. 982.1 - *IEEE Standard Dictionary of Measures to Produce Reliable Software*, 1988
7. IEEE Std. 982.2 - *IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software*, 1988
8. ANSI/IEEE Std. 983 - *IEEE Guide for Software Quality Assurance Planning*, 1986
9. ANSI/IEEE Std. 990 - *IEEE Recommended Practice for Ada as a Program Design Language*, 1986
10. ANSI/IEEE Std. 1002 - *IEEE Standard Taxonomy for Software Engineering Standards*, 1987
11. ANSI/IEEE Std. 1008 - *IEEE Standard for Software Unit Testing*, 1987
12. ANSI/IEEE Std. 1012 - *IEEE Standard for Software Verification and Validation Plans*, 1987
13. ANSI/IEEE Std. 1016 - *IEEE Recommended Practice for Software Design Descriptions*, 1987

14. IEEE Std. 1028 - *IEEE Standard for Software Reviews and Audits*, 1988
15. ANSI/IEEE Std. 1042 - *IEEE Guide to Software Configuration Management*, 1988
16. ANSI/IEEE Std. 1058.1 - *IEEE Standard for Software Project Management Plans*, 1987 [PAR approved for revision October 1993]
17. ANSI/IEEE Std. 1063 - *IEEE Standard for Software User Documentation*, 1989.

The following standards in this series were approved:

- IEEE 1045, *Software Productivity Metrics*, 1992
- IEEE 1061, *Standard for a Software Quality Metrics Methodology*, 1992
- IEEE 1016.1, *Guide to Software Design Description*, 1993
- IEEE 1219, *Standard for Software Maintenance*, 1993

Standards under development in this series include:

- IEEE P1016.2, *Guide to Software Design Descriptions*
- IEEE P1044, *Standard for Classification of Software Anomalies* (formerly entitled *Classification of Software Errors/Faults/Failures*)
- IEEE P1059, *Software Verification and Validation*
- IEEE P1062, *Software Acquisition*
- IEEE P1074, *Software Life Cycle Processes*
- IEEE P1228, *Software Safety Plans.*

Development of international software engineering standards by ISO/IEC JTC1/SC7 on Software Engineering is still in its early stages. The near-term emphasis will be on establishing a foundation on which to build future standards. The following standards projects are underway in SC7's working groups [Ref. Edelstein 1991]:

- WG1—Symbols, Charts, and Diagrams
  - Conceptual framework for software development diagrams
  - Charting techniques for software development and maintenance
  - Conventions for use of symbols and icons in software systems
- WG2—System and Software Documentation
  - Guidelines for documentation of computer-based systems
- WG4—Tools and Environments
  - Evaluation and selection of CASE tools
- WG5—Reference Model for Software Development
  - Reference model
  - Reference model overview
- WG 6—Evaluation and Metrics
  - Software quality characteristics
  - Software quality management
  - Requirements/design/testing, etc.
- WG 7—Life Cycle Management
  - Software configuration management
  - Software life cycle management
- WG 8—Integral Life Cycle Processes
  - Transfer of information between life cycle phases
- WG 9—Classification and Mapping
  - Reference model—mapping of relevant information systems engineering standards.

A definition of software engineering life cycle processes has been progressed to CD status. It is intended to serve as a reference point in discussions between suppliers and clients, and is not an attempt at defining a method. SC7 plans to develop a technical report on *Software Process Assessment*. Detailed definitions of generic processes are also underway, such as configuration management. SC7 has progressed to the IS level two documents entitled *Software Product Evaluation, Quality Characteristics and Guidelines for Their Use* (ISO 9126, 1991); and *User Documentation and Cover Information for Consumer Software Packages* (ISO 9127, 1988).

Just as the OSI reference model organized activity on communications standards, a reference model is being developed by SC7/WG9 to organize the work on products and standards for software engineering. It is called the Standardization Framework for Software Engineering and is planned to help identify where standards are needed to create open systems in the field of information systems engineering. A study in 1991 by the Commission of the European Community (CEC) concluded that because of the importance of the information industries in the European Community (EC), actions must be taken to remove the barriers to free trade in this sector. The report established the need for a consistent and integrated set of information systems engineering standards to open up the closed markets. It also introduced the concept of OpenISE, information systems engineering without barriers to competition and free trade. European Community for Standardization (CEN) WG63, which began meeting in February 1992, is charged with developing an action plan for European standards in information systems engineering. SC7/WG9's framework will play an important part in helping WG63 select and prioritize the standards needed for OpenISE. The framework has only recently reached stability. [Ref. OSN 1993e]

International activity that will affect software development is the standardization of quality management systems. ISO 9001, *Quality Systems,* represents a concise, generic description of the essential elements of management systems for assuring quality in development, production, and qualification with emphasis on the "what" over the "how." ISO 9000, Part 3: *Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software*, was approved by international ballot and adopted by TC 176 in November 1990. [Ref. Edelstein 1991]

A new ISO standard on software quality was recently approved: ISO 12119, *Information Technology: Software Packages: Quality Requirements and Testing*, 1993. It was developed from the German standard DIN 66285:1990 that defines the conditions for granting a quality mark (*Guetezeichen* software). Currently, more than 100 products exist with a quality mark.

There are currently no standards specifically for the development of expert systems. It is not clear that the development of expert systems will need to follow a different or unique process model.

The ESPRIT project "accueil de logiciel futur" aims to provide a knowledge-assisted software process model on top of the PCTE. [Ref. Brettnacher 1988]

Development methods tend to be proprietary and not subject to standardization. However, one IEEE project (P1152), *Standard for Object Oriented Programming Language and Environment,* is developing a standard based on the SmallTalk programming language and environment.

4.4 Standards for Programming Interfaces

Formal standardization of programming interfaces includes new work being conducted by SC21. A special working group (SWG) conducted a year-long effort (June 1992 to June 1993) to identify application program interface (API) activities in relation to the areas of standardization for which SC21 was responsible, with the view of basing its work on the framework provided by the Reference Model for Open Distributed Processing (CD 10746) and recognizing work taking place outside SC21. The report of the SWG [SC21 N 8045] and its recommendations [SC21 N 8052] on gathering information about priorities and plans for standardization of programming interfaces were accepted by SC21 and forwarded to JTC1.

SC21 dissolved this SWG and replaced it with another to receive liaisons from other groups in response to the June 1993 report [SC21 N 8045], to prepare appropriate responses, and to prepare SC21 contributions to a joint working group (JWG) between SC21 and SC22, should JTC1 approve its formation. SC21 welcomed establishment of active liaison with X/Open and requested C-liaison status for X/Open on the topic of APIs and related architectural frameworks. The initial meeting of the new SWG was held in November 1993.

Fast-track DISs are expected to be submitted by IEEE on common ASN.1 object management APIs for X.400 and Directory Service APIs; X.400-based electronic messaging API; and Directory Service API. APIs are addressed in more detail in Sections 15.1.3 and 15.2 in connection with application portability.

4.5 Assessment of Coverage by Standards

There are international standards for most, but not all, of the commonly used programming services. Although ISO and the US Government have adopted ANSI X3.159, Programming Language C, there are potential compatibility problems between C and C++. The other standards are stable. However, Ada is undergoing a revision process and some aspects of the current language may not be upwardly compatible with its successor, Ada 9X. Moreover, COBOL is currently limited in real-time, operating system, and communications components.

There is no standard set of guidelines for using the features of the Ada programming language; without guidance, applications written in Ada may have unpredictable portability. Ada bindings are needed for many interfaces, such as graphical user interface (GUI) toolkits, OSI Application Layer functionality, CASE Data Interchange Format (CDIF), Standard Generalized Markup Language (SGML), X.25, and Transmission Control Protocol/Internet Protocol (TCP/IP). They have been completed for GKS (ISO 8651-3), PHIGS (ISO 9593-3), and SQL (ISO 9075:1992), and are at the DIS level for GKS-3D (DIS 8806-3) and CGI (DIS 9638-3). Ada bindings for X, SQL, and IRDS (ISO 10728 WDAM 2) are underway. IEEE P1003.5 is currently defining Ada bindings only to POSIX.1 and not to the other POSIX standards. P1003.20 is reported to be developing an Ada binding to POSIX real-time extensions.

All fourth generation languages (4GLs) are proprietary. Portability of 4GL products requires open standardization of languages and bindings.

Standards have not been developed for languages used for certain technologies and application areas. These areas might include languages used in artificial intelligence (standards for LISP and Prolog have been developed but not for other languages) and used for interfaces to specific COTS/NDI software. LISP is more popular in the United States while Prolog is more popular in the United Kingdom and Europe, posing potential interoperability problems.

Standards for software development environments, including CASE tools and environments, are in the early phases of development. Some are currently restricted to interfaces between tools while others address entire environments. Standards are needed for integrated (computer-aided) software engineering environments (ISEEs) and tools. These include systems and programs for automated assistance in the development and maintenance of software, such as tools for requirements specification and analysis, for design work and analysis, for creating program code, for testing, for documenting, for prototyping, and for group communication. The interfaces among these tools include services for storing and retrieving information about systems and exchanging this information among the various system development environment components. ECMA's PCTE and associated reference model is widely supported by vendors in Europe. The Ada Programming Support Environment (APSE) specifications can be mapped to this reference model. The work of defining interfaces among various software components is still incomplete and in a state of flux. For example, there is as yet no consensus on the type of data model necessary to support the information structures for the environment. The extent to which environments such as PCTE and CAIS can evolve and be tailored is unknown. Moreover, CAIS is suffering from a dearth of conforming commercial products. Tool interfaces based on commercial products may lack flexibility.

Standards for KBS do not exist. Software repository standards to facilitate reuse do not yet exist. This could have an adverse effect on a COTS/NDI acquisition strategy by making NDI software difficult to identify.

Software engineering standards that address the software development process and development methods, and ultimately software quality, are in the early phases of the international standardization process. It will be at least 3 years before a foundation for these standards is established. To date, none addresses the development of expert systems.

5. USER INTERFACE SERVICE STANDARDS

5.1 Requirements for User Interface Services

User interface services specify the human-computer interface (HCI), terminal management services, and interactions with virtual terminals. Such standard interfaces are needed to ensure a high degree of application portability and to provide a consistent look and feel across multiple implementations. An overview of standards for user interfaces is given in Table 3.

The user interface services provide a consistent way for the people who develop, administer, and use a system to gain access to applications programs, operating systems, and various system utilities. An information system architecture addresses not only the technical features of the user interface but also the human engineering considerations. User interface services address client-server operations, object definition and management, window management, and dialog support.

HCI standardization is based on, but extends beyond, the selection of a commercial off-the-shelf (COTS) graphical user interface (GUI). While the GUI provides a standard application program interface (API) and style guide, application designers are only provided with recommended generic approaches. Varying interpretations of the GUI style guide and of users' needs can still result in dissimilar HCIs among applications developed by independent organizations. Adding to the standardization problem is the fact that COTS GUI packages do not address special issues such as map graphics. [Ref. DoD HCI Style Guide 1992]

5.2 Standards for User Interface Services

Human-computer interfaces comprise two levels of standardization. One level is the specification of how computer system elements shall interface to display terminals and other output devices with a capability for human interaction. The second level is the look, feel, and layout of the display screens, keyboards, and other elements of the workstation that define the way information is displayed and how the user interacts with that information.

Table 3. Status Overview of Key Human Computer Interface Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
X Window Sys.	●	○	○	●	●	●	
IEEE P1295.1	●	●	○	○	○	●	○

Key: ● High Evaluation; ○ Average Evaluation; Blank Low Evaluation

Source: [Ref. APP 1993]

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

5.2.1 HCI Standards Organizations

The standards work in ISO/IEC covers both levels of HCI. These standards activities seek to:

- Provide consistency—in screen and keyboard layout, terminology, semantics, user action, and syntax—across and within manufacturers, systems, and applications
- Enhance comfort and well-being
- Enhance usability[21]
- Assist in product procurement and evaluation.

Specifically, ISO/IEC JTC1/SC18 (Document Processing and Related Communication, formerly Text and Office Systems) has a working group, SC18/WG9 (User System Interfaces and Symbols), that is developing standards to support keyboard layout, user interfaces, cursor control, and icons (e.g., symbols) to be displayed. In addition, the Ergonomics Technical Committee (TC159) of ISO is addressing, through SC4 (Signals and Controls) and WG5 (Software Ergonomics and Man-Machine Dialogue), standards for dialogue interface, coding, formatting, menus, and usability assurance. Other areas of standardization related to the user interface of information systems being addressed by ISO are [Ref. Bevan 1989]:

- Documentation (JTC1 SC7/WG2)
- Software quality characteristics (JTC1 SC7/WG3)
- Text interchange (JTC1 SC18/WG4)
- Terminal management (JTC1 SC21/WG4)
- Form Interface Management System (FIMS) (JTC1 SC22)
- POSIX (JTC1 SC22/WG15)
- Commands for interactive text searching (TC46/SC4)
- Software quality assurance (TC176 SC2/WG5).

Other groups working on HCI standards include [Ref. Reed 1991]:

- ITU-TS Study Group X, Working Party 1, Man-Machine Language
- Human Factors Society, Human Computer Interaction Committee
- ANSI X3V1.9, User System Interfaces and Symbols
- IEEE Steering Committee on User Interface (SCWUI)
- IEEE Project 1201, Window Interface for User and Application Portability
- Open Software Foundation (OSF)'s Motif Graphical User Interface (GUI)
- UNIX International (UI) OPEN LOOK GUI [Ref. SUN 1990]
- Information Industry Association
  - Voice Messaging User Interface Forum (VMUIF)
  - Voice/Fax User Interface Forum (VFUIF).

5.2.2 Visual Display Terminal (VDT)

Work has been underway for several years on the hardware user interface standards, now known and approved as Human Factors Society (HFS)/ANSI 100-1988, *Human Factors Engineering of Video Display Terminal Workstation Standard.* To date, however, there has been relatively little work on software user interface standards. The HFS Technical Standards Common

---

21 As used in SC18/WG5, usability of a product is defined as the degree to which specific users can achieve specified goals in a particular environment effectively, efficiently, comfortably, and in an acceptable manner.

Human-Computer Interaction was formed in 1985 to evaluate the feasibility of software user interface standards. It has submitted a fully reviewed document on menu-based dialogue design to the ISO Working Group on Software Ergonomics (TC159/SC4/WG5). [Ref. Reed 1991]

SC18/WG9 seeks to develop a user interface standard that would address names of basic objects and actions, user guidance, dialogue interaction, and graphical symbols used on screens. The standard is DIS 9995: *Information Technology - Keyboard Layouts for Text and Office Systems*. The current parts represent a recombination of material formerly in 21 parts:

- DIS 9995-1 (Part 1), *General Principles Governing Keyboard Layouts*
- DIS 9995-2 (Part 2), *Alphanumeric Section*
- DIS 9995-3 (Part 3), *Common Secondary Layout of Alphanumeric Zone of Alphanumeric Section*
- DIS 9995-4 (Part 4), *Principles Governing the Placement of Characters and Symbols on Keys*
- DIS 9995-5 (Part 5), *Editing Section*
- DIS 9995-6 (Part 6), *Functional Section*
- DIS 9995-7 (Part 7), *Symbols Used to Represent Functions*
- DIS 9995-8 (Part 8), *Allocation of Letters to the Keys of a Numeric Keyboard.*

SC18/WG9 has also distributed working drafts of two components of an as-yet unnumbered standard for icons used on screens. The standard is intended to apply to systems implementing the desktop metaphor, although icon systems suitable for other application fields may be future subjects of standardization. [Ref. Billingsley 1990] ANSI X3V1.9 is the US Technical Advisory Group to WG9.

TC159 SC4/WG5 is developing a standard (ISO 9241) for VDTs that addresses office task requirements, visual requirements, keyboard ergonomics, work place design and environment, surfaces and filters, use of color and graphics, non-keyboard input devices, usability, coding, formatting, and terminology. The status of the parts to ISO 9241, *Ergonomic Requirements for Office Work with Visual Display Terminals*, is as follows:

- ISO 9241-1 (Part 1), *Introduction*, 1992
- ISO 9241-2 (Part 2), *Task Requirements*, 1992
- ISO 9241-3 (Part 3), *Visual Display Requirements*, 1992
- DIS 9241-4 (Part 4), *Keyboard Requirements*
- CD 9241-5 (Part 5), *Workstation Layout and Postural Requirements*
- CD 9241-6 (Part 6), *Environmental Requirements*
- CD 9241-7 (Part 7), *Display Requirements with Reflections*
- CD 9241-8 (Part 8), *Requirements for Displayed Colors*
- CD 9241-9 (Part 9), *Requirements for Non-Keyboard Input Devices*
- WD 9241-10 (Part 10), *Dialogue Principles*
- CD 9241-11 (Part 11), *Usability Statements*
- CD 9241-12 (Part 12), *Presentation of Information*
- WD 9241-13 (Part 13), *User Guidance*
- CD 9241-14 (Part 14), *Menu Dialogues*
- WD 9241-15 (Part 15), *Command Dialogues*
- WD 9241-16 (Part 16), *Direct Manipulation Dialogues*

- WD 9241-17 (Part 17), *Form-Filling Dialogues*
- XX 9241-18 (Part 18), *Question and Answer Dialogues* (CD expected in 1994)
- XX 9241-19 (Part 19), *Natural Language Dialogues* (CD expected June 1994).

5.2.3 Virtual Terminal (VT)

VT standards (ISO 9040 and 9041) define a communications protocol between a terminal and its host in terms of a conceptual terminal, where the mapping from the conceptual terminal to the physical device is an implementation issue outside the standard. The VT standards specify how terminal systems and host applications on a network can communicate without requiring one side to know the terminal characteristics of the other side. The capabilities and constraints of different types of terminal-application dialogues are defined by a VT profile.

Several classes of display and data manipulation capabilities will eventually be addressed by VT standards [Ref. OSN 1989b]:

- Basic class, for textual data in a rectangular array of character boxes
- Forms class, similar to the basic class, but with the ability to define fields with control over data entry
- Graphics class, for geometric data such as lines and circles (as defined, for example, in GKS)
- Text class, for structured data such as provided by Office Document Architecture (ODA) data streams
- Image class, for bit-mapped displays.

The 1990 revision of ISO 9040 and 9041 incorporates an amendment (AM1) to define enhanced access rules, structured control objects, blocks, fields, and reference information objects.

Amendment 2 [SC21 N 7243, June 1992] for ISO 9040/9041 enhances the capability of the virtual terminal environment (VTE) by use of the Association Establishment and Negotiation functions, extends the set of objects and operations provided by the Data Transfer function, and enhances error handling capabilities of the service provider. Amendment 2 provides additional functionality for ripple mode editing (insertion, deletion, and copy operations for a Display Object), exception reporting (provides mechanisms by which non-fatal exception conditions may be reported by the VT service provider to both VT users), and retention of VT context across Negotiation (retention of the information stored in selected VT Objects—Display Object and Control Objects—to be retained between successive VT environments within the lifetime of a VT association).

ISO 9041-2, *VT Protocol Implementation Conformance Statement (PICS) Proforma* reached IS status in February 1992. In addition, registration authority procedures have been developed for the VTE and VT Control Objects: ISO 9834-4 and ISO 9834-5, respectively. Finally, a guide to VT standards has been developed by SC21/WG5 [SC21 N 3365, December 1988]. *Conformance Test Suite for the VT Protocol - Part 1: Test Suite Structure and Test Pruposes* (ISO 10739-1), August 1992, has also been developed.

Intercom Data Systems (IDS) of Woking (UK) claims the first commercial implementation of the VT standard: VirtuOSI. [Ref. OSN 1993b]

VT profiles are being developed by two regional workshops: the EWOS and the NIST OSE Implementor's Workshop (OIW). EWOS is working on synchronous-mode profiles that are based on a two-way exchange with a single display object requiring the exchange of an access token. EWOS profiles include [Ref. SGFS N 100 1992]:

- FVT1 nn, *Register of VTE-profiles,* pDISP 11184
- FVT2 nn, *Register of Control Object Type Definitions,* DISP 11185
- FVT3 nn, *Register of Assignment Type Definitions,* pDISP 11186.

The OIW is developing asynchronous-mode profiles. These are based on a character-by-character interworking, in which there are two display objects, but the user at each end is allowed to update only one of the objects. OIW profiles include Telnet, Transparent, Forms, Scroll, Paged, and X.3/X.28/X.29 [packet assembler/disassembler (PAD)]. Individual parts of the profiles for Virtual Terminal are identified in Table 4.

Table 4. Registration Profiles (FVTs) and Application (AVTs) for Virtual Terminal

pDISP 11184	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles (DISPs expected in 1994 or 1995)
Part 1:	FVT 121 - S-mode Forms VTE Profile, 1993
Part 2:	FVT 122 - S-mode Paged VTE Profile, 1993
Part 3:	FVT 111 - A-mode Telnet Profile
Part 4:	FVT 112 - A-mode Scroll VTE Profile
Part 5:	FVT 113 - A-mode CCITT X.3 PAD Interworking
Part 6:	FVT 114 - A-mode Transparent VTE Profile
Part 7:	FVT 115 - A-mode Generalized Telnet VTE Profile, 1993
DISP 11185	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects (Parts 1-11 are DISPs; the others are pDISPs)
Part 1:	FVT 211, FVT 212, Sequenced and Unsequenced Application Control Objects, 1993
Part 2:	FVT 213, FVT 214, Sequenced and Unsequenced Terminal Control Objects, 1993
Part 3:	FVT 215, FVT 216, Application RIO Record Locating Control Object and Terminal RIO Record Notification Control Object, 1993
Part 4:	FVT 217, Horizontal Tabulation Control Object, 1993
Part 5:	FVT 218, Logical Image Control Object, 1993
Part 6:	FVT 219, Status Message Control Object, 1993
Part 7:	FVT 220, Entry-control Control Object, 1993
Part 8:	FVT 221, Forms Field Entry Instruction Control Object (FEICO) No. 1, 1993
Part 9:	FVT 222, Paged Field Entry Instruction Control Object (FEICO) No. 1, 1993
Part 10:	FVT 231, Forms Field Entry Pilot Control Object (FEPCO) No. 1, 1993
Part 11:	FVT 232, Paged Field Entry Pilot Control Object (FEPCO) No. 1, 1993
Part 12:	FVT 251, Terminal Conditions Control Object No. 1
Part 13:	FVT 2111, Waiting Time Control Object (pDISP expected 1995)
Part 14:	FVT 2112, Printer Control Object, 1993
Part 15:	FVT 2113, Field Definition Control Object, 1993
Part 16:	FVT 2114, Terminal Signal Titles Control Object, 1993
Part 17:	FVT 2115, Form Help Text Control Object, 1993
pDISP 11186	ISPs FVT 3nn - Virtual Terminal Basic Class - Register of Assignment Type Definitions
Part 1:	FVT 321, Font Assignment Type No. 1
DISP 11187	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles (Parts 3-10 are pDISPs; DISPs expected in 1994 or 1995)
Part 1:	AVT 22, S-mode Forms Application Profile, 1993
Part 2:	AVT 23, S-mode Paged Application Profile, 1993
Part 3:	S-mode ISPICS Requirements List No. 1
Part 4:	S-mode ISPICS Requirements (IPRL) List No. 1, Supporting Layers List No. 1
Part 6:	AVT 13, A-mode Scroll Application Profile
Part 7:	AVT 14, A-mode CCITT X.3 PAD Application Profile
Part 8:	AVT 15, A-mode Transparent Application Profile
Part 9:	AVT 16, A-mode Generalized Telnet Application Profile, 1993
Part 10:	AVT 17, A-mode ISPICS Requirements List No. 1

In May 1991, SC21/WG5 generated a document for study and comment on the possibility of supporting interactive access to ODA data structures through an extension of the VT protocol. [Ref. SC21 N 6227 1991]

5.2.4 Terminal Management (TM)

SC21/WG5 initiated a program for developing standards f, directed at support for multi-function workstations, which has now been terminated. The role of TM was to support the control and manipulation of logical devices typically associated with workstations. Logical devices were defined in TM to provide a mapping between transferred data such as ODA documents and the physical devices such as a workstation screen, taking into account control information such as synchronization and the use policy of a particular application. TM was related to work on Document Transfer and Manipulation (DTAM, ITU-TS); user interface standards (SC18); Forms Interface Management System (FIMS, SC22); and window management (SC24).

The TM standard was to have consisted of three parts: *TM Model* (CD 10184-1.2), *TM Service* (WD 10184-2), and *TM Protocol* (WD 10184-3). The first, *TM Model*, progressed to second CD status in June 1991 and was expected to progress to DIS in July 1992 and IS in July 1993. CD status for the other two was expected in December 1992; however, in August 1993 the project was cancelled. [Ref. SC21 N 8081 1993] Reasons for the cancellation include lack of resources and the fact that X-Windows is now progressing on a fast-track ballot.

5.2.5 Status of X-Windows

The X-Windows standard effort,-based user interface standard, began as a de facto standard developed at the Massachusetts Institute of Technology). It was developed by Project Athena and the Laboratory for Computer Science at MIT with funding and participation by Digital Equipment Corporation (DEC) and IBM. [Ref. McCartney 1987] Currently in Version 11 (Release 5), X-Windows sets a standard to provide portability of information across different hardware and operating systems. In contrast to the kernel-based architecture of traditional windowing systems, it has a network-based architecture. [Ref. Stoffel 1989; Oldenburg 1989]

X-Windows is a graphical user interface standard that enables a user to view and gain access to multiple computer applications from a single window or multiple windows on a display screen. X-Windows is based on a client-server architecture that allows applications and resources to be distributed across a network. The X-server is a software program resident on a user's display unit that acts as an intermediary between the user and applications running on a local or remote system. The applications are referred to as X-clients. These applications access the display unit by sending messages to the X-server, which is then able to perform the two-dimensional drawing of lines, shapes, and text. The X-server also maintains complex data structures such as specific windows, cursors, and fonts that can be referenced and used by applications. Input from the keyboard and/or mouse is collected by the X-server and passed to local and/or remote applications for processing. [Ref. IGOSS 1993]

Some features added in Release 5 include:

- Internationalization that allows programmers to develop applications that can be adapted to different native languages, local customs, and character encodings
- PHIGS Extension for X (PEX)
- Font server to manage fonts separately from the X server.

Release 6 is expected to emphasize three-dimensional extensions to X and embed the ability to drag or drop icons onto programs, but it is not expected for some time. Since MIT believes it is time X developments moved into the commercial arena, the X Consortium is planned to become a not-for-profit company funded by membership dues. [Ref. OSN 1992l]

The strategic direction in ISO for OSI support of windowing environments was embedded in the Terminal Management project, whose cancellation was due, in part, to the rapidly growing demand for the X-Windows system. This demand is being satisfied by the use of X-Windows clients and servers collocated in the same machine or over LANs using protocols such as TCP/IP. Some large user communities are now trying to run X-Windows over wide area networks (WANs) and in some cases plan to install TCP/IP networks in competition with the emerging OSI networks based on ISO protocols. [Ref. SC21 N 4189 1989]

An efficient OSI compatible way of supporting the X-Windows System is needed. While it would be preferable from the standards point of view to rewrite X-Windows completely, this would require developmental effort and dedicated expertise that does not appear to be available. Further, by the time any such standard becomes complete, it would likely be too late to gain acceptance. Instead, in April 1991, ANSI X3 announced the approval of a new project on X-Windows System Data Stream Definition. Part 4 of this draft standard (X3.219) represents the mapping of Version 11 of X-Windows (X11) onto OSI services using the OSI Application Layer naming and addressing conventions. [Ref. X3 1991i] The work has progressed well, and a four-part standard has gone out to ballot in the X3H3 group. The four parts are:

- Part 1, *Functional Specification*
- Part 2, *Data Stream Encoding*
- Part 3, *Keysym Encoding*
- Part 4, *Mapping onto OSI Services.*

Parts 1 through 3 define the X-Windows data stream definition, and Part 4 defines the mapping (using an OSI skinny stack) of X-Windows data streams onto OSI application service elements (e.g., ACSE) and Presentation Service. When X3.219 is approved by ANSI, it will be submitted to ISO for fast track balloting through SC24. [Ref. OSN 1992l; IGOSS 1993]

Because X11 has limited two-dimensional (2D) graphics capabilities, a consortium of organizations under the auspices of MIT has developed X3D-PEX, an extension to the X11 standard that supports the Programmers' Hierarchical Interactive Graphics System (PHIGS) and the three-dimensional version of the Graphical Kernel System (GKS-3D). [Ref. Clifford 1988] PHIGS and GKS are discussed in Sections 8.2 and 8.3, respectively.

FIPS-158, *X-Windows User Interface,* was approved in May 1990 as a US mandatory standard. It is based on Release 3 of Version 11 of the MIT X-Windows de facto standard and is compatible with Release 4, which is currently available from most vendors. Since the de facto standard is now in Release 5, NIST plans to issue FIPS 158-1 soon. [Ref. Kuhn 1991]

The Display Industry Association (DIA) recently released the Alpha Windows Standard for displaying applications software in windows on low-cost terminals. The Alpha standard is an alternative to the X-Windows standard where graphics are not required. The specification was completed in August 1991 [Ref. OSN 1992g], and the first commercial shipments of terminals and software complying with the Alpha Windows standard arrived in July 1922.

Although the X-Windows system is a standard for user interfaces in a distributed environment, it has no single GUI component. It was a deliberate policy of the writers of X to

provide a generic mechanism that could be used to create particular user interfaces. A GUI is built from two main parts:

- The toolkit that provides windows on the screen
- The window manager that gives the user control over the display.

Motif and OPEN LOOK, two GUI products that extend the user interface, were competing to become the de facto standard. [Ref. OSN 1992l]

A new body is forming to promote X-Windows. The X Industry Association (XIA) will likely focus on marketing X-Windows and competing with Microsoft's Windows NT and the Alpha Windows standard. XIA's exact relationship with the X Consortium is not yet clear. [Ref. OSN 1993a]

The US DoD is planning to recommend a GUI that provides a consistent *look and feel* across all DoD corporate information applications and environments. The GUI is to be based on FIPS Pub 158 (X-Windows/X11) and will incorporate features and functionality developed through open, public-consensus forums, such as the IEEE P1201 committee. A recommendation for the GUI has been developed by a multi-Service/Agency working group and is contained in the draft version of the *Recommended Department of Defense Human Computer Interface (HCI) Style Guide for Corporate Information Management*, July 1993 (see Section 5.3). [Ref. CALS/CE 1992]

5.2.6 User Interface Reference Models

FIPS-158 comprises the first three layers (Layers 0-2) of the User Interface Reference Model developed by NIST. [Ref. Kuhn 1990] The NIST Model consists of:

- Layer 0: Data Stream Encoding
- Layer 1: Data Stream Interface, X-Library (Xlib)
- Layer 2: Subroutine Foundation, X-Toolset (Xt) Intrinsics
- Layer 3: Toolkit
- Layer 4: Dialogue
- Layer 5: Presentation
- Layer 6: Application.

Layer 0 is an X-Protocol for messages between client and server. It equates with ANSI X3.196, *X11 Data-Stream Encoding for Window Management*. Layer 1 is a library interface that provides a C language interface to the X-Protocol. Layer 2 consists of basic functions for controlling windows and acts as a tool kit for builder. [Ref. Kuhn 1990]

NIST Reference Model Layers 3 through 5, while not part of FIPS-158, are the subject of IEEE projects. Layer 3 is equivalent to IEEE Project 1201.1, *Uniform Application Program Interface, Graphical User Interfaces*, Draft 3, February 1992. It defines a uniform application program interface that can be used by implementors of GUI applications to develop computer programs that are portable across multiple window systems and user interface toolkits, such as OSF/Motif, OPEN LOOK, Microsoft Windows, OS/2 Presentation Manager, and Apple Macintosh.

IEEE Working Group P1295.1 is working on a source code level interface to an X-Window System Toolkit graphical user interface environment based on the OSF Motif Application Environment Specification User Environment (see Section 5.2.7). It includes a C language API consistent with IEEE P1201.2. The draft standard is entitled: *Draft Standard for*

Information Technology - X-Windows System Graphical User Interface, Part 1: Modular Toolkit Environment (IEEE P1295.1). P1295.1 provides a toolkit of functions and objects for developing the API for a GUI. Use of P1295.1 in conjunction with FIPS 158 implementations of X-Windows will provide a complete GUI but without the management capabilities that can be provided in dialog and presentation tools (Layers 4 and 5) such as User Interface Management Systems (UIMS). NIST expects P1295.1 to advance from de facto to de jure status in a relatively short time. [Ref. APP 1993, pp. 30-31] It passed its first ballot with only three negative votes and was expected to reach formal IEEE standard status as early as December 1993.

Layers 4 and 5 are addressed respectively by the User Interface Language and the UIMS work of IEEE Project 1201.3 and are still in the research stage. IEEE has formed a study group, but not a working group, for these efforts.

The GUI part of the IEEE P1201 Reference Model is not included in the NIST Reference Model. The GUI is the subject of IEEE Project 1201.2, *Driveability Guide*, which provides a recommended practice for minimal commonality for window systems (see Section 15.1.3.3). [Ref. Kuhn 1991] A draft was balloted in July 1992, and a standard was expected mid-1993.

5.2.7 OSF/Motif

The OSF/Motif GUI is the result of OSF's request for technology (RFT) process, which solicited input from the worldwide computer industry for GUI technology. OSF/Motif was released in July 1989 and incorporates technologies from Digital Equipment Corporation, Hewlett-Packard, and Microsoft. It is currently in Release 1.2.

OSF/Motif offers user-oriented PC-style behavior and screen appearance for applications running on any system that can support X-Windows System, Version 11, Release 5. It comprises an API consisting of a toolkit and User Interface Language (UIL). In addition, its window manager offers a standard environment for manipulating application windows. The OSF/Motif environment provides Native Language Support (NLS) consistent with the NLS solution proposed in the X/Open XPG3. The UIL can fully support display of 16-bit and compound strings, including all character sets standardized by the X Consortium, to provide localization in Asian and European languages. [Ref. OSF 1990a]

OSF has produced a validation suite and, as of May 1993, there were nine certified implementations of Motif 1.2. Motif is a candidate for X/Open's fast-track process and for standardization as IEEE 1295.1.

OSF plans to produce a significant new version of Motif in 1993 or 1994, has a parallel project on interoperability, and is investigating a move to a "next-generation user environment," called UEC II, sometime after 1995. A current major concern is compatibility with Windows, since Motif is based on the X-Windows protocol and Windows is not. Without the ability to integrate the two, the majority of PC users have no way to access applications through Motif without running an X terminal as one application under Windows on their PC. Even when doing this, there is no easy way to exchange information between the two sets of applications. [Ref. OSN 1992c]

An April 1993 Department of the Air Force Electronic Systems Center (ESC) Memorandum mandates the use of Motif Version 1.1 in conjunction with X-Windows as the Graphical User Interface for all new programs and modifications to existing systems. This applies to command center and management information systems, not embedded systems. [Ref. ESC 1993]

5.2.8 OPEN LOOK

OPEN LOOK, jointly developed by Sun Microsystems and AT&T is another implementation-independent GUI specification. On first release, OPEN LOOK could be considered technologically more advanced than its OSF counterpart, Motif, since it included such features as icon drag and drop handling as an integral part. Moreover, utilities such as file manager, calendar manager, and print manager are more fully integrated in OPEN LOOK. However, as a result of the recent Common Open Software Environment (COSE) agreement [Ref. OSN 1993f] between five major UNIX suppliers, Sun agreed to support Motif as its standard GUI and significantly reduced its efforts on the development of an OPEN LOOK-based standard. Among other COSE agreements, the suppliers have agreed on a common UNIX "dashboard," based on Motif to pull the UNIX industry together and strengthen X/Open's position as a broker of industry standards. In August 1993, the working group developing the OPEN LOOK standard formally withdrew, leaving Motif as the only X based standard effort. [Ref. Hurd 1993]

5.2.9 Form Interface Management System (FIMS)[22]

The Form Interface Management System (FIMS) is being developed by SC22/WG18. FIMS (DIS 11730) is a high-level user interface tool that builds on top of the windowing and menu features in GUI tool kits, but at a higher level of abstraction. The distinctive features that FIMS gives a form are its record level interface, validation, and built-in dialog management model.

FIMS achieves a high degree of program/device independence by allowing a form to be customized for a device, taking advantage of its special features, rather than being limited to a least common denominator. It is possible to create a form that looks natural on block-mode terminals, workstations, and laser printers.

FIMS is optimized for operation in a network, where the user interface often sits on a front-end node. Dialog management facilities allow efficient user interaction. Since the API is at the record level, network traffic is minimized. [Ref. Frantz 1992]

5.2.10 Extensible Virtual Toolkit (XVT)

Version 2.0 of XVT, available from XVT Software, Inc., was published January 1990. XVT allows applications to be portable among various window systems including Motif, OPEN LOOK, MS-Windows, Macintosh, OS/2 Presentation Manager, and CIOS Presentation Manager. It does not provide window and graphics support, only a common interface that applications can use to access the features of the underlying window and graphics system. IEEE P1201.1 has adopted XVT and the base document for its work, and several major software/hardware vendors have chosen it as the API to be used on UNIX platforms. [Ref. APP 1992]

5.2.11 Intelligent HCI

The Computer-Human Object-Oriented Reasoning Interface System (CHORUS) is a generic architecture for intelligent interfaces. Its features include an attempt to isolate and implement the main functionalities of an intelligent interface, multimode input, interpretation of user input in terms of goals and plans, and adaptation of the interface features to the individual user. [Ref. RNLA 1994, p. 335]

---

22 "The Standards Reporter," in *Open Systems Standards Tracking Report*, Volume 1, No. 1, October 1991, p. 2.

5.3 HCI Style Guidelines

The following documents have been developed to provide guidelines for the use of HCI standards and COTS products meeting such standards (civil standards are listed first):

- NIST User Interface System Reference Model
- FIPS 158, User Interface Component of *Applications Portability Profile*, Version 1, May 1990
- IEEE P1201.2, *Recommended Practices for Graphical User Interface Driveability*, IEEE, Draft 2, May 1992
- *OPEN LOOK Graphical User Interface Application Style Guidelines*; Sun Microsystems, Inc., AT&T, Second Printing, June 1990
- *OSF/Motif Style Guide*, Open Software Foundation, Release 1.0, 1990
- *Human Computer Interface Style Guide*, Center for Information Management, US Defense Information Systems Agency, Version 3.0, 31 July 1993, UNCLASSIFIED
- *DoD Intelligence Information Systems (DODIIS) Style Guide*, DODIIS Management Board, June 1991
- *Air Force Intelligence Data Handling System Style Guide*, US Air Force Intelligence Agency, October 1990
- *Defense Intelligence Agency (DIA) Standard User Interface Style Guide for Compartmented Mode Workstations* (known as the DIA Style Guide), DIA, DIA Memorandum U-15,284/DSE-3, 31 May 1983
- STANAG 2019, *Military Symbols for Land-Based Systems;* Army Field Manual (FM) 101-5-1, *Operational Terms and Symbols*, October 1985; and DIAM 65-xxx, *Standard Military Graphics Symbols*, Draft, DIA, 1990
- *Human Factors Guidelines for the Army Tactical Command and Control System Soldier-Machine Interface*, US Army by Pacific Northwest Laboratories, August 1990.

The US DoD HCI Style Guide is based on the above documents. Indeed, it is an adaptation of the *DoD Intelligence Information Systems (DODIIS) Style Guide*, and it is based on the NIST User Interface System Reference Model. It presents guidelines for application development within Layers 0 through 5 of the Reference Model as follows:

- Layer 0 (Data Stream Encoding): Network Protocol from X-Windows
- Layers 1 and 2 (Data Stream Interface and Subroutine Foundation): Library Functions from X-Windows
- Layer 3: Subroutine Foundation: Toolkit standards that support the window management application program interface (API)
- Layers 4 and 5 (Presentation and Dialog): User Interface Design Language (UIDL) and User Interface Management System (UIMS)—these define the "look and feel" of the GUI.

The purpose of an HCI style guide is to provide a common framework for HCI design and implementation. It is to be used to standardize interface implementation options, enabling all applications to appear and operate in a reasonably consistent manner. Specifying the appearance, operation, and behavior of software applications will support such operational objectives as higher productivity, reduced training time, and reduced development time. The emphasis of the guidelines is on considerations for features and functions such as system start-up, security issues, and map graphics.

5.4 Assessment

Of all the service groups, standards for the user interface services are some of the least mature. This area suffers from a general lack of standards for toolkits and UIMS and at the API level itself. API directions likely to be taken over the next 5-10 years are uncertain. GUIs remain in the research stage. Standards for window management are only emerging. While X-Windows still has not reached the stage of becoming an international standard, work is progressing. X-Windows has wide support in the United States and elsewhere, but the implementations are not standardized. Moreover, most of the X-Windows functionality is available only at a low level, too low for most application programming. The Extensible Virtual Toolkit (XVT) is one of many toolkits that provide a higher level API to window system functions that are window-system independent. There are as yet no standards for the "look and feel" for application software for the upper layers (Presentation and Dialog) of the user interface system reference model (see Section 5.3). User interface services may be one area in which de facto standards must be used in lieu of international standardization.

6. DATA MANAGEMENT SERVICE STANDARDS

6.1 Requirements

Data management standards support the storage, control, distribution, management, and allocation of simple data (text and numeric information) as well as complex data (complete documents, maps, charts, images, and multimedia objects). An overview of the status of data management service standards is given in Table 5.

One or more standard query languages can be used as the basis of the peer-to-peer protocol for the exchange of data between information systems. More than one type of data structure (e.g., relational, hierarchical, image/map oriented) may be required. The information transfer services are primarily constrained by finite communications bandwidth and security.

Managing Data Complexity. Enabling users to pull information they need in an ad hoc way from diverse sources requires database interoperability. SQL-based database management systems are in widespread use for this purpose. Future developments that enhance portability include "transparent access" database exchanges and encapsulating existing databases into object-oriented "objectbases." [Ref. RNLA 1994, p. 27]

Security and Exchange Mechanisms. Security is discussed in Section 11.2. Exchange mechanisms provided by the communications standards for network services are discussed in Chapter 9. The data management services will provide mechanisms to accurately represent the meanings and relationships of the information items to be managed. These mechanisms include the database system, the conceptual schema, and information system domains. For each type of data structure to be supported, these mechanisms will provide a standard way of representing the data, including support for common data definitions. (The definitions as well as the data would be standardized during the implementation phase of a specific information system.) An example of one type of support that could be provided is a data dictionary system, which could be used by information systems to maintain common data definitions and representations.

Table 5. Status Overview of Key Data Management Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
IRDS	○		●	●	○		
SQL	●	●	●	●	●	●	●
RDA	○		○		○		○

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

Key: ● High Evaluation; ○ Average Evaluation; Blank Low Evaluation

Source: [Ref. APP 1993]

Another example is the data definition language (DDL) that may be provided with a database system or language. The DDL must be rich enough in its forms of expression to have attributes required of both commercial and military systems. For example, it needs to have the capability to recognize several types of hierarchy for data classification and compartmentalization and be trusted to permit access by users with varying levels of authorization for these classification levels and compartments.

6.1.1 Definitions for Data Management Concepts

Several concepts underlie data management services; these may be informally defined as follows. Persistent data are data that are not limited to a single service request. Metadata are data about data, specifying the structure, format, location, or constraints that apply to data. A database is a collection of persistent data (which may include metadata describing itself or other database) managed in accordance with the metadata contained in a schema. A schema is a collection of metadata that describes and constrains a database (a schema cannot be altered without ensuring that appropriate changes are made to the database that it describes). A database controller is a (standardized) processor that provides access to and management of a (local) database in accordance with the (local) schema describing that database (Database Language SQL provides database controller services). Local distribution data is a local source of descriptions of remote data. A distribution controller is a (standardized) processor that provides access to and management of both local and remote data and metadata. (Formal definitions are provided in the *Reference Model for Data Management,* ISO/IEC 10032). [Ref. SC21/WG3 N 1557 Rev 1993]

6.1.2 Information System Requirements for Data Management

The following operational requirements for support of data management for information systems have been identified by ISO/IEC 10032, *Reference Model on Data Management (RMDM)*:

- Access control
- Information systems life cycle support
- Configuration management, version control, and variants
- Concurrent processing
- Database transaction management
- Performance engineering
- Referencing data
- Extensible data modelling facilities
- Support for different data modelling facilities at the user interface
- Audit trails
- Recovery
- Logical data restructuring
- Physical storage reorganization.

6.1.3 Partitioned, Partially Replicated Database Capability

Data transfer services in future information systems are expected to be provided by a Partitioned, Partially Replicated Database (PPRDB) capability. Partitioning means that the entire information system database is segmented into disjoint parts that are held at geographically separate locations. Some of the parts of the information system database are copied or replicated at other locations to ensure survivability or to provide more rapid local access. A partitioned, partially replicated database provides sufficient flexibility for efficient exchange of information in a manner

that minimizes usage of communication by permitting either "push" access (for updates) or "pull" access (for queries).

6.1.4 Conceptual Schema

A common conceptual schema is needed to define all information system data related to information exchange. The information system database will be segmented or partitioned into replication domains, each owned and managed by a specified subfunctional area. Each replication domain has one master copy and may have other copies referred to as slave copies. A single component would be able to access some, but not all, of the master and replication domains.

6.1.5 Domains

Each domain comprises two parts. One part (domain details) provides the characteristics and control information for the domain. Examples of possible domain details are: name, owner, home information system component for the master domain, list of permitted users, component addresses for the replication domains, and security classification parameters. The other part of a domain (domain data) provides the values of each data item. The representations of some features of a domain, such as data item characteristics, data relationships, and data dictionaries, are implementation dependent and have therefore not been specified.

6.1.6 Distributed and Federated Database Systems

Distributed Database System. A distributed database may be considered as a collection of data in which an application process accessing the data does not require explicit connections to the database environment. In particular, an application process functions in such a way that does not need to take into account how data are distributed or in which database environment data are processed. [Ref. SC21/WG3 N 1557 Rev 1993]

Distribution Controllers. Distributed database environments may differ as to the extent of fragmentation and replication of data and the scope of individual operations and transactions. A distribution controller is introduced into distributed database systems to provide the services to support those aspects of managing data in a distributed environment that are not provided by each local environment. [Ref. SC21/WG3 N 1557 Rev 1993]

Federated Database System. In some cases of distributed database systems, there are no prior constraints involving the need to support particular kinds of operations or interfaces to existing components. In these cases, the capabilities of the distribution controller determine the degree of management of data that is possible. In cases of design and construction of an information system in which there are a number of pre-existing database systems, an additional design criterion is the extent to which the component database systems retain a degree of autonomy for their own operation. Related design choices include (1) decisions for each user of an original component database system to decide whether to continue to access their data directly through the local database system or through a distribution controller; and (2) deciding the scope of constraints, whether they remain local to a database environment or involve data distributed in many database environments. The general situation, in which there is some combination of component autonomy and distributed data management is known as a federated database system. [Ref. SC21/WG3 N 1557 Rev 1993]

Distributed Access. A distributed information system may include a number of autonomous database systems whose data are to be shared, possibly on an ac hoc basis, by application processes. In this situation, cooperative data management is limited to providing for

remote access to data. The distribution controller can provide such application processes with services that enable some degree of distributed processing, such as transactions encompassing multiple database environments. One particular requirement for the ad hoc use of data is the need for access to appropriate data definitions, providing both a syntax (representation) and semantics (meaning) of the data. [Ref. SC21/WG3 N 1557 Rev 1993]

Distribution Data. Distribution data describe the way that data are distributed in a distributed database system. Since operation of a distributed database may involve exchange of distribution data, a standard is required for its definition. A standard schema for distribution data is needed that is consistent with and supportive of the information system requirements noted in Section 6.1.2 (above) and the special requirements for distributed information systems given below. There may also be a need to define a set of standard services to make use of the distribution data.

Special Requirements. Requirements from ISO 10032 to support data management in a *distributed* information system (in addition to those identified in Section 6.1.2) are the following: distribution control, database transaction management, communications, export/import, distribution independence, system autonomy, and recovery of a distributed database. Four additional requirements are under study in ISO: distributed deadlock management, query processing, distributed query optimization, and heterogeneity (encompassing data modelling facilities, database management system implementations, and multiple schema representations and interpretations).

6.1.7 Required Services

The following basic services appear to be required:

- Data definition—provides a common understanding between systems on the attributes and meaning of data.
- Local queries—queries that can be satisfied by a data item or a set of items as specified in parameters supplied in the query, subject to authentication of the requestor's identity before issuing the data, such that the data resides in either a master or slave copy at the location where the query is made.
- Remote queries—transfers, from a remote master or slave copy, of a data item or a set of items as specified in parameters supplied in the query, subject to authentication of the requestor's identity before issuing the data, from a location other than the one where the query originated.
- Consistency control—ensures that any updates to values of data items in a slave copy ultimately become the same as the values in the master copies of the relevant domain; consistency control also ensures that update transactions are applied in the correct order.
- Local updating—provides for changing the values of a data item or set of data items for a domain, where the master copy is held at the same location as the one where the update originated.
- Local slave updating—provides for changing the values of a data item or set of data items for a slave domain, but without replication of the updates.
- Remote updating—provides for changing the values of a data item or set of data items for a domain, where the master copy is at a remote location; these operations are subsequently directed to all slave copies of the relevant domain.
- Integrity of replicas—ensures that each replica, together with deferred updates, can be used to replace the master domain in the event of a system failure.

- Management of distribution—supports the partitioning and partial replication of the databases.
- Recovery from failure—provides mechanisms to decide that there has been a failure, allows recovery from failure, and permits a slave copy to become a master copy.
- Master-slave management—permits a slave to become the master and new slave copies to be designated dynamically.
- Database statistics—provides status and usage data for the system manager.
- Database initialization—provides for the creation and loading of initial values of a database and its replicas when the system is initialized.
- Standard knowledge base—documents knowledge information.

In addition, the following management services appear to be required:

- Create domain—creates a new, empty domain, either as a master copy or for use as a replication copy of a domain.
- Delete domain—deletes a domain and erases all data in that domain. (When applied to a master copy it will delete all associated replication copies.)
- Transfer domain—causes, when proceeding to normal completion, the master of the domain to become a slave copy and the slave copy at a designated replication component to become the master.
- Assume domain—provides for change of ownership of a domain.
- Unassume domain—provides the capability to resolve the situation in which more than one information system component has exercised assumption of the same domain by designating another domain as the master.
- Amend domain—provides for changing the characteristics of a domain, such as the list of users or the replication list, by the owner or other authorized user.
- Details domain—provides for query of the details or characteristics of a domain by an authorized user.
- Copy domain—copies the entire contents of a domain, both characteristics and data, to a replication copy. (Space for the copy is first created by "create domain.")
- Restore domain—allows the owner of a domain to recreate the data in the master copy of the domain by copying it from a replication copy, in support of data recovery after failure.
- Advise domain—allows an information system component to be interrogated to see if it holds a copy of a domain. (This permits components who have lost and then reestablished communications to find out whether the replication list is correct.)

Some options for standardizing the appropriate features of domains are inherent in the discussions in the sections that follow. Some services being evaluated to provide database operations (not yet adopted) imply implementation of a relational database architecture. Examples of database operations are: select, update, delete, insert, project, product, union, intersect, difference, divide, join, and equijoin.

6.2 Standards for Database Services

This section primarily addresses the technical aspects of data management. The procedural aspects of data management are addressed in Section 6.3. The Reference Model for Data Management described below applies to both the technical and procedural aspects.

6.2.1 ISO Reference Model of Data Management (RMDM)

The *Reference Model of Data Management* is ISO 10032. Development of the RMDM began in 1988, and it was approved with IS status in January 1992.

ISO 10032 includes in the scope of data management the description, creation, modification, use, and control of data in information systems. The model provides a framework for identifying interfaces; positioning interfaces relative to each other; identifying facilities provided at each interface; identifying the process that supports each interface and, where appropriate, the specific data required for this support; positioning the use of the interfaces in terms of the information system's life cycle; and identifying the binding alternatives associated with each interface. The concepts defined in the model may be used to define the services provided by particular database management systems or data dictionary systems. The data management field of application concerns any user—human or applications program—who wants to request services for management and storage of information in a persistent manner.

SC21/WG3 is preparing a technical report, *Application of the Reference Model of Data Management* (formerly entitled, *Tutorial for Reference Model of Data Management*), that will address the following topics [Ref. IST 21 1534 1988]:

- Tutorial aspects for the Reference Model of Data Management
- Analysis of current database standards in terms of the Reference Model concepts
- Analysis of data management services using data flow diagrams
- Description of current database standards with respect to the requirements of the Reference Model.

A rapporteur meeting on the technical report was held during November to December 1993. PDTR text is expected in July 1995, DTR in 1996, and TR in 1997.

6.2.2 Data Definition and Manipulation Language Standards

There are now two data manipulation language standards approved by ISO: NDL[23] and SQL.[24] Both are standards of ANSI and are US Federal Information Processing Standards (FIPS).

6.2.2.1 Database Language NDL

Database Language NDL (ISO 8907, ANSI X3.133-1986, FIPS 126) is an outgrowth of 1978 Conference on Data Systems Languages (CODASYL) specifications using a network model for a DDL and a data manipulation language (DML). NDL is characterized, in part, by extensive use of logical pointers. These pointers support such facilities as FIND NEXT (push down in a stack) and FIND OWNER (pop up in a stack). The specification work was conducted from 1981 to 1986 by the ANSI X3H2 Database Committee. No follow-on standards activities are being conducted by ISO or ANSI for NDL. [Ref. Deutch 1987; Gallagher 1988] Implementations supporting NDL are rare. The existing ANSI and ISO NDL standards will likely be withdrawn unless some user or vendor establishes a requirement for its continued existence. [Ref. Gallagher 1991a] Although NDL was reconfirmed as an international standard in 1993, the UK requested that the matter be reconsidered at the Yokohama Meeting in June 1993. When SC21/WG3 met in

---

[23] NDL is not an acronym; historically, the term derived from the concept of a network data language.

[24] SQL is also not an acronym; historically, the term derived from the concept of a structured query language, but today represents much more.

Yokohama in June 1993, it recommended that the NDL standard not be withdrawn. [Ref. SC21 N 7764 1993; SC21 N 8123 1993]

6.2.2.2 Database Language SQL

SQL (ISO 9075, ANSI X3.135-1986, FIPS 127) is based on a relational database model; the specification work was conducted from 1982 to 1986 by the ANSI X3H2 Database Committee. Future work in the standards for database management systems by ISO and ANSI X3H2 will be on distributed database processing (e.g., remote data access protocol) and extensions to SQL. The first ISO standard for SQL was ISO 9075:1988.

Both ISO and ANSI worked closely together and in parallel on a second edition of SQL (known as SQL2 during its development), which achieved IS status in 1992. This standard is an upward compatible enhancement of two existing SQL standards: *SQL with Integrity Enhancement* (ANSI X3.135-1989; ISO 9075:1989) and *Database Language - Embedded SQL for COBOL, FORTRAN, PL/1,* Ada *, and C* (ANSI X3.168-1989). The technical content of ISO 9075:1988 is retained as a level of the 1992 standard. The Integrity Enhancement Feature provides for check clauses, default clauses, and referential integrity constraints. Two addenda to ISO 9075:1992 are in progress:

- WDAD 1, Addendum 1: *SQL Call-Level Interface (CLI)*, Working Draft, January 1993 [SC21 N 7596] PDAD status recommended by WG 3.
- WDAD 2, Addendum 2: *Persistent SQL Modules*, Working Draft, January 1993 [SC21 N 7597] PDAD status recommended by WG 3.

The ANSI standard X3.135-1986 SQL allows for two levels of compliance. Level 1 is a core standard that leaves many areas open to implementation definition. Level 2 contains many extensions over Level 1, but Level 2 still has a large number of options for implementation. Examples of facilities found in Level 2 but not in Level 1 are [Ref. Martin 1989]:

- Atomic transactions with respect to recovery
- Eighteen-character identifiers
- Table-name qualification by user-name
- Indicator variables
- Outer references
- Keyword ALL allowed in query-specifications, sub-queries, and set functions
- Updatable query-specification definitions
- Statements atomic with respect to database changes
- Not equal to comparisons (<>)
- Escape characters in the LIKE predicate
- REAL, DOUBLE PRECISION, and NUMERIC data types
- WITH CHECK OPTION on a view definition
- WITH GRANT OPTION on a privilege definition
- DISTINCT with AVG, MAX, MIN, and SUM.

In February 1990, FIPS 127 was revised (FIPS 127-1) to incorporate integrity enhancement and embedded SQL. FIPS 127-1 also documents guidelines and considerations for procuring SQL systems. It was revised again (FIPS 127-2) in February 1992 to adopt SQL2.

NIST has established a test suite and formal testing service which provide a basic SQL conformance validation. The NIST SQL Test Suite, Version 4, July 1993 consists of over 450 tests, and NIST issues certificates of validation. [Ref. Sullivan 1992] The test suite measures

conformance to required features of FIPS PUB 127-2. The 1992 SQL standard is divided into three bands: entry level, intermediate level, and full.[25] The FIPS 127-2 adds a fourth band: transitional. The NIST SQL Test Suite tests only the entry level. NIST anticipates that the transitional level tests will be available in 1995.[26] NIST publishes a quarterly list of FIPS-validated processors. Validation summary reports (VSR) are issued for each test conducted, regardless of when certificates are issued. [Ref. APP 1992]

Work has already begun on a third edition of ISO 9075 (known during its development as SQL3). The SQL3 working draft is contained in SC21 N 6931, June 1992, and the statement and content of the project is in SC21 N 8091, June 1993. SQL3 is currently in its 4th working draft. CD text is expected in July 1994, DIS in July 1995, and IS in July 1996. SQL3 includes many facilities important to engineering and scientific applications, including object data management, hierarchies of class definitions, inheritance, complex types, user defined data types, generalized triggers and assertions, export/import of databases; and support for database management [Ref. DRA 1994]. SQL3 would incorporate the following features:

- Generalized triggers (similar to IF...THEN statements; based on a condition of data, not time)
- Generalized assertions (given a certain condition, to trigger integrity checks on the database to be done before and after validation on values in the database)
- Recursive expressions (these allow an open-ended subordinate assertion, such as to completely search a tree; currently, only finite queries to specified levels are permitted)
- Escape from SQL to call external features
- Basic capability for user-defined data types (the only structure in SQL is a table; this allows the user to declare a domain separate from a table)
- Support for subtables, provided through inheritance and generalization features
- Appropriate support tools for object-oriented and knowledge-based systems.

An analysis of comments received on the SQL3 WD showed general agreement on a requirement to restructure. The following structure was proposed by the database language group (DBL) in November 1992. SQL3 would be separated into an SQL family of standards consisting of the following [Ref. SC21/WG3 N 1450 1992]:

- A framework document that describes the relationship and positioning of the "core" and all "packages"
- A base document that specifies the "core" and those packages whose definitions are best expressed as part of the base document
- A set of separate documents, one for each package not contained in the base document.

SQL3 has object-oriented extensions that include user-defined abstract data types, addressing methods, object identifiers, subtypes and inheritance, polymorphism, type templates, and integration with existing facilities. Base data type in SQL3 include fixed-length and variable-length character strings, fixed-length and variable-length bit strings, fixed and floating point numerics, dates, times, time stamps, intervals, Booleans, and enumerations. Base data types can be used in connection with generator types to create new data types. It is expected that the following generator data types, known as complex object support, will be added to the SQL3

---

[25] "NIST Certifies Oracle 7 for SQL Conformance," by John Stein Monroe, *Federal Computer Week*, October 18, 1993, p. 30.

[26] Per telephone conversation 27 October 1993 with Joan Sullivan, NIST (301) 975-3258.

specification: List, Set, and Array. It is possible that other generator data types, such as those specified in the Common Language-Independent Data (CLID) type specification (e.g., Choice, Record) will also be added to the SQL3 specification. [Ref. SC21 N 8205 1993]

SQL/MM. SQL applications have the requirement to use the same abstract data types across different application areas, thereby promoting interoperability and sharing of data and encouraging performance optimization over a manageable collection of types. The multi-part standard, referred to as *SQL Multimedia and Application Packages* (SQL/MM), would specify packages of SQL abstract data types and consist of 11 parts: Framework, Full Text, Still Graphics, Animation, Still Image, Full Motion Video, Audio, Spatial (2D and 3D), Seismic, Music, and Mathematical Structures. The SQL/MM project plan is contained in SC21 N 8205, September 1993. Since the standard is proposed as a "companion" standard to SQL3, its standardization is dependent upon the standardization of SQL3. The target date for the Framework, Full Text, Still Graphics, and Still Image parts is 1996. Other parts will follow in subsequent years. [Ref. SC21 WG3 N 1298 1992; SC21 N 8205 1993] Working drafts of the first three parts have been circulated, for which CDs are expected in June 1994:

- Part 1: *Framework* [SC21/WG3 N 1647, September 1993]
- Part 2: *Full-Text* [SC21/WG3 N 1613, September 1993]
- Part 3: *Spatial* [SC21/WG3 N 1614, September 1993].

The resource requirements necessary to forward this proposed new work item to JTC1 for letter ballot were met in December 1992. Since the new work item proposal for SQL/MM just met the criteria for acceptance into the JTC1 program of work, SC21 has been asked to determine the true level of support and participation for this work item. [Ref. SC21 N 7744 1993] Several SC18/WG3 activities on ODA are relevant to SQL/MM work (see Section 7.1.1).

A working paper for X3H2 [SC21 WG3 N 1286; ANSI X3H2-92-8, November 1991] outlines requirements for an SQL External Repository Interface so that non-SQL data repositories can make their data available, in simplified but standard form, to SQL systems or SQL applications.

A CALS (see Section 7.1.4) Phase III requirement calls for "intelligent" DBMSs. SQL3 intends to provide facilities for managing object-oriented data and for forming the basis of "intelligent" DBMSs. Of particular importance are many of the proposed SQL3 features to the STEP (see Section 7.2.1) because of that standard's unique data modelling and data access requirements. Existing and planned features in SQL3 may not satisfy all STEP requirements, but they should provide an appropriate base from which many requirements can be suitably addressed. [Ref. Gallagher 1990]

6.2.2.3 Export/Import Facilities for SQL and IRDS

A new work item in SC21, on export and import for SQL and IRDS [SC21 N 5137] is planned to be a three part standard entitled, *Data Management Export/Import Facilities*, with three parts:

- Part 1: *Framework*
- Part 2: *Facilities for SQL*
- Part 3: *Facilities for IRDS.*

The new work item, Generic Data Management Export/Import, was not accepted. A revision focused on SQL and IRDS was accepted in 1991 [JTC1 N 1484] and later restructured

(June 1993) as a multi-part standard. Although the parts will be progressed separately, CD status is expected in July 1994, DIS in July 1995, and IS in July 1996.

6.2.2.4 Common Language-Independent Data Type

WG3 has noted that the Common Language-Independent Data Type (CLID; ISO 11404) definition (see Section 4.3.1) of a Table differs significantly from that of a Table in SQL. Since SQL has been standardized by ISO since 1986, and SQL tables are in widespread use, the SQL concept, well founded in relational theory, appears to be a strong candidate as a common language-independent data type. Therefore, DBL passed a motion authorizing a paper [SC21/WG3 N 1452] defining the differences between the existing SQL and CLID concepts of a table, be submitted to SC21/WG3 and to SC22/WG11 for the purpose of recommending that CLID either adopt the SQL concept or drop Table from their specification. [Ref. SC21/WG3 N 1452 1992]

6.2.2.5 SQL Ada Module Description Language

The SQL Ada Module Description Language (SAMeDL) (CD 12227) effort is the subject of standardization by SC22/WG9. SAMeDL is a language which, when processed by an appropriate tool, generates the SAME abstract module and other code necessary to access a particular database management system. [Ref. AJPO 1992] The standard is currently in DIS balloting.

6.2.2.6 SQL Access

An historical problem with SQL has been the creation of non-standard versions resulting in interoperability problems, especially in distributed environments. In 1989, several mid-tier database vendors recognized the problem and organized the SQL Access Group (SAG) to resolve some of the SQL incompatibilities. SAG works on middleware (see Section 13.5.1) standards for both accessing data and navigating networks, but progress has been slow. Vendor contributions to SAG include Microsoft's Open Database Connectivity (ODBC)[27] specification and the Independent Database API (IDAPI) by Borland International, IBM, and Novell. [Ref. Stahl 1993]

6.2.3 Remote Data Access (RDA)

Scope of RDA. In many environments, there are heterogeneous database systems that need to be interconnected. The Remote Database Access (RDA) standard provides the communication mechanisms to integrate such systems. It provides independence such that a RDA user can use the same front end to access different database systems, and a single database may be shared by different workstations. RDA specifies a two-way transfer syntax as well as the semantics for database operations. [Ref. Tang 1992; IGOSS 1993]

RDA addresses distributed database processing in a client-server environment. An RDA client, modelled by an application process running in some workstation, reads or updates a remote database system. The interface between a RDA client and the RDA service provider can operate in either a synchronous or an asynchronous mode. A RDA server, which is attached to a database system, responds to requests from a RDA client. Both the RDA client and the RDA server are RDA service users. [Ref. Tang 1992]

---

27 The ODBC specification allows developers of client software to connect applications to a variety of database servers by writing to one SQL application programming interface (API). [Ref. OSN 1993m]

RDA[28] is an ISO standard to facilitate access to databases from intelligent workstations and from other database systems. It is essentially a (standard) generalization of certain operations of database systems, file servers, and document servers. RDA will allow, with a minimum of technical agreement outside the interconnection standards, the interconnection of applications and database systems from different manufacturers, under different managements, of different levels of complexity, and exploiting different technologies. Since an application may itself be a database system, RDA can be used to support multi-database system interworking.

RDA service is designed to provide all possible valid data manipulation functions on any database. The functions needed (and available) depend on the structure and content of the database, so the definition of these functions must be accomplished at run time (not explicitly coded into software). Thus, RDA allows data management language operations to be defined and named (actually numbered), so that they can be repeatedly invoked later in an application and association.

RDA Standards. The ISO standard for RDA (ISO 9579) defines the format and meaning of messages that support this application. RDA uses the following common application service elements (ASEs) to provide the communications services: Association Control Service Element (ACSE; ISO 8649 and ISO 8650); Commitment Concurrency and Recovery (CCR; ISO 9804 and ISO 9805); and ROSE (ISO 9072). RDA can be viewed as a composition of ACSE and CCR with a specialization of the ROSE.[29] RDA needs no specific protocol of its own; it only requires additional sequencing rules and a method for handling violations of them. The Abstract Syntax Notation standards (ISO 8824 and 8825) are used in the Presentation Layer to define structures (data types) and rules for encoding structures so that the structures can be transmitted.

ISO 9579 is based on work of the ECMA Technical Committee on Databases, ITU-TS, and ISO SC18. ECMA TR30 (December 1985) was the starting point for RDA, and ECMA TR31 initially defined the concepts, notation, and connection-oriented mappings for remote operations. ISO 9579 has three parts and several draft amendments:

- ISO 9579-1 (Part 1): *Generic Model, Service, and Protocol*, March 1993 [SC21 N 7689]
  - WDAM 1, Amendment 1: *Generic RDA*, August 1992 [SC21 N 7202] (PDAM expected June 1993; DAM in June 1994; AM in June 1995])
- ISO 9579-2 (Part 2): *SQL Specialization*, March 1993 [SC21 N 7703]
  - PDAM 1, Amendment 1: *Support for SQL 2*, September 1993 [SC21 N 8307]
  - WDAM 2, Amendment 2: *Support for Stored DBL Statements*, October 1990 [SC21 N 5138] (a new work item accepted in August 1991; rapporteur meeting January 1994; PDAM expected July 1995)
- CD 9579-3 (Part 3): *SQL PICS Proforma*, October 1993 [SC21 N 8087] (formerly entitled *IRDS Specialization)* (editing meeting January 1994)

The remote operations philosophy is based on object modelling in which the functionality of an object is modelled as a set of operations available at its interface. Object modelling also includes the notion of object classes, subclasses, and property inheritance. In RDA these concepts are used to define a generic RDA, which defines a class of remote database access applications, and specific RDAs, each of which defines a subclass of RDA applications. Those properties

---

28 Discussion taken from *Remote Database Access Tutorial*, SC21 N 1927, 28 July 1987; and DP 9579-1, 29 March 1990 [SC21 N 4282].

29 Application service elements ACSE, CCR, RTSE, and ROSE are discussed in Section 9.11.3.

common to all RDA applications are defined in the generic RDA. Those that relate to subclasses are defined in RDA specializations.

The generic RDA (ISO 9579-1) can support any data management language. One of the specific RDAs is a specification for the Database Language SQL. Other specific RDAs to be developed in the near future are also expected to be based on the relational approach. The relational data management language was chosen because it supports complex selection functions and multi-record operations for updating and deletion. This enables the RDA to accomplish selection processing in the database server (the place where the data are stored). This reduces the amount of unneeded data that are transferred to the client (user) and thus minimizes use of communications. [Ref. SC21 N 1927 1987]

SQL Specialization (ISO 9579-2) defines the service and protocol for access to databases and supports the data manipulation functions of SQL. This is done through specifying the transfer syntax for specific data manipulation functions, as provided for in ISO 9075 for SQL database systems. The elements of the SQL (or any other) specialization are definitions for [Ref. SC21 N 3342 1989]:

- Data resources available as a result of establishing a dialogue and any constraints on opening and closing further data resources
- Data structure of a class of data objects supported
- Permissible classes of operations upon the objects
- Representation of all operations in an abstract syntax
- Representation for data passed as parameters for these operations.

The SQL specialization for RDA (ISO 9579-2) augments the generic RDA (ISO 9579-1) so that the two parts together define the following:

- Capabilities of an SQL database server that supports dialogues with clients
- Model of dialogues between the SQL database server and remote users
- Model of a dialogue between an RDA client and an SQL server
- Abstract service interface for the RDA SQL ASE that models the communications facilities supporting interaction between the SQL client and the SQL server
- RDA SQL ASE protocol to support the RDA SQL service
- Characteristics of application contexts that include the RDA SQL ASE
- Application contexts that support remote database access using SQL, specifically the RDA Basic Application Context and the RDA TP Application Context.

An RDA application may be implemented in conjunction with the Basic Application Context or the TP Application Context. The Basic Application Context includes only the ACSE and provides a one-phase commit protocol. The TP Application Context provides a two-phase commit that allows updates at multiple remote sites in the same transaction. Some options for use o the Basic Application Context (interoperability parameters) are [Ref. IGOSS 1993]:

- Immediate execution, which immediately executes the database operation
- Stored execution, which permits optimization by allowing database operations to be defined and stored in the database server and to be executed one or more times during the RDA dialogue possible with different parameters for each execution
- Status, which allows the status of a database operation to be queried
- Cancel, which allows a database operation to be cancelled.

Other RDA Projects. In October 1990, a new work item proposed creating an addendum to ISO 9579 entitled, *RDA Support for Stored DBL Statements* [SC21 N 6257]. In November 1991, WG3 recommended approval for this new work item and it was registered as a PDAM in May 1992. However, a May 1992 joint-WG3/RDA and WG3/DBL meeting voted not to progress the draft document in SC21/WG3 N 1243 to CD status. Most recently, in the absence of an Editor and Target dates, SC21 is recommending the cancellation of this project. [Ref. SC21 N 7728 1993]

A PDTR, *Remote Database Access Tutorial* [SC21 N 3343, January 1989], was planned for June 1993; however, the project has been cancelled [Ref. SC21 N 8081].

The RDA Rapporteur Group has reviewed the proposed extensions for character sets in ASN.1 and associated encoding rules against WG3 requirements and found that they meet most of the requirements [SC21/WG3 N 1248].

The SQL Access Group (see Appendix F, Section 3.30) and X/Open (see Appendix F, Section 3.35) are working on a joint RDA specification.

A June 1991 report, *Interim Report on the Feasibility of Profiling Database Enquiry* [IST21 N 2880] extends the scope of an earlier project on RDA to database enquiry (DBE) for all user-oriented database operations, which support and control the creation, modification, and retrieval of data in a database and the maintenance of the logical structure of the database. The report concludes that work should begin to define profiles for DBEs that would cover user access facilities and procedures, information presentation, communication, transaction management, and database management. The work would require additional base standards (e.g., RDA SQL specialization, user interface standards, and distributed database management standards) and extensions to the taxonomy of TR 10000-2. Work on DBE is being undertaken by the EWOS Expert Group on Database Enquiry.

Expert Group on Database Enquiry (EG-DBE). In February 1992, the European Workshop for Open Systems (EWOS) established an Expert Group (EG) on DBE. The work began on two fronts: (1) examination of the profile taxonomy defined in ISO TR 10000, and (2) development of the extensions necessary to accommodate DBE. [Ref. SC21 WG3 N 1345 1992] The objects of the EG-DBE are to

- Define a taxonomy for the development of functional standards in the area of database enquiry taking into account the methodology given by ISO/IEC TR 10000 and the approaches described and referenced in the report of EWOS PT 014; a draft of an RDA taxonomy was discussed in October 1993 and revised for approval of the EG-DBE in January 1994 [EWOS/EG-DBE/93/055].
- Develop profiles for DBE, together with complementary conformance testing specifications
- Establish user requirements and priorities for the development of DBE profiles; a draft User Requirements for RDA was discussed in October 1993 [EWOS/EG-DBE/93/088].

DBE is intended to be interpreted in a wide sense, encompassing the communications elements implied by remoteness, the DBMS elements implied by database, and also user interfaces.

The formal initial work program of EG-DBE contains the following:

(1) Development of taxonomy for DBE requirements

(2) Development of profiles for access to relational databases

(3) Development of profiles for access to databases containing large structured objects (e.g., ODA documents)

(4) Development of test specifications for profiles

(5) Establishment of user requirements for DBE profiles and of additional DBE scenarios.

In March 1993, EWOS requested an S-liaison between the EWOS/EG-DBE and ISO/IEC JTC1 SC21/WG3. [Ref. SC21 N 7651 1993] In October 1993, the EG-DBE noted [EWOS/TA/93/0425] widespread interest in Internet convergence and work in X/Open on RDA over TCP/IP.

6.2.4 Information Resource Dictionary System (IRDS) Standards[30]

Stable IRDS Standards. An IRDS is a system that provides facilities for creating, maintaining, and accessing an Information Resource Dictionary (IRD) and its IRD definition. There are two stable international standards for IRDS:

- ISO 10027:1990, *IRDS Framework*, June 1990
- ISO 10728, *IRDS Services Interface*, 1993 [SC21/WG3 N 1466]
  - PDAM 1: *C Language Binding* [SC21 N 8088, June 1993]
  - WDAM 1: *Ada Language Binding*, September 1993 [SC21 N 8203].

The IRDS *Framework* provides a common basis for developing IRDs, which are sharable repositories for the definition of the information resources relevant to all or part of an enterprise. The *IRDS Services Interface* specifies an interface that gives any program full access to all IRDS services, through whatever external call interface is provided by the language in which the program is written.

Information resources. Information resources governed by an IRD may include:

- Data needed by the enterprise
- Computerized and possibly noncomputerized processes that are available for presenting and maintaining such data
- Available physical hardware environment on which such data can be represented
- Organization of human and physical resources that can make use of the information
- Human resources responsible for generating that information.

The IRDS standard does not provide a standard definition of all the above kinds of information. Rather, it provides a framework for defining such information in which the information can be represented and managed. The content of an IRD can be compared with the content of a typical application database—an application database contains data of relevance to the day-to-day operation of an enterprise. The difference is that the data are at a higher level (metadata or data about data) and may include such entities as data item types, data files, computer programs, and subsystems.

An IRDS is used to control and document an enterprise's information resources. ISO 10027, *IRDS Framework*, defines a number of concepts that are basic to data management. A *database* is a collection of interrelated data stored together with controlled redundancy according to a schema to serve one or more applications. *Database integrity* is the consistency of a collection of data in a database. *Export* is the function of extracting information from an IRDS and packaging it to an export/import file. *Import* is the function of receiving data from an export/import file into an IRDS. An *IRD* is a part of a repository managed by an IRDS in which the information

30 Portions of the discussion of IRDS are taken from ISO 10027, *IRDS Framework*.

resources of an enterprise may be recorded. A *value* is an abstraction with a single characteristic that can be compared with other values and that may be represented by an encoding of the value. A *data modelling facility* is a set of data structuring rules and an associated set of data manipulation rules. An *application schema* is a set of definitions that control what may exist at any time in an application.

IRDS framework, facilities, and interfaces. The *IRDS Framework* identifies the kinds of data, together with the major processors and their associated interfaces, and the broad nature of the services provided at each interface. Aspects addressed by various IRDS standards include programming language dependence, interface style, data modelling facility used, and data interchange format. Examples of processor interface styles are programmatic (such as a procedure call interface, consisting of a sequenced set of parameters and associated binding rules for the CALL statement in a programming language); syntax for execution time interpretation; and service convention (a standard set of programming language independent conventions for specifying parameter lists and service primitives for use in an open systems environment). Examples of alternative styles for human interfaces are: panels (abstract screen formats), concrete syntax (such as a command language), and graphics.

An abstract syntax is the specification of a service (such as for an interface style) by using notation rules that are independent of the encoding techniques used to represent them. An abstract syntax may be used to define a set of services without prescribing any linguistic form to be used when each service is initiated or invoked. (See Section 9.10.1 for discussion of ASN.1.)

Examples of data modelling facilities are those based on standard database languages such as NDL or SQL, based on a non-standard database language, specific to a standard programming language (such as COBOL or PL/1), specific to a non-language standard (such as OSI Directory services), or which are non-standard data modelling facilities (such as entity-relationship modelling). Each data modelling facility is an intrinsically independent means of representing data and possibly the services that may be specified for such data.

Three types of support can be provided for a database using international standards. One is using standardized services at an interface, in which the contents of some part of the IRD are defined, together with the services by which those contents may be accessed and manipulated. The second type of support is by standardizing in precise terms the content of some part of an IRD according to some prescribed data modelling facility. The services that may be performed on that data may or may not be implicit in the general data manipulation services associated with that data modelling facility. The third type of support is the use of a standard data interchange format, designed to facilitate the interoperability of several real systems by standardizing the formats of the various kinds of messages sent from one real system to another. A data interchange format may be specific to an application.

IRDS provides for two types of user interfaces: a menu-driven (panel) interface and a command language interface. The panel interface provides for a structured path of screens (i.e., panels) by which an inexperienced user can execute IRDS functions. The command language may be used in either an interactive or batch mode.

IRDS, including the command language and panel interfaces, is specified in terms of entities, relationships, and attributes. The entities represent or describe the concepts and data objects about which values are to be stored in the database. Relationships are binary associations between two entities (e.g., one contains the other). Attributes represent the properties of an entity or relationship. Each relationship and attribute is assigned a specific type. Entities can be

compared if they have a common attribute with a common type. Ordered sets of attributes, called attribute groups, are also provided in IRDS. The IRDS schema that defines and controls what is permitted in a data dictionary is also defined using entities, relationships, attributes, and attribute groups. IRDS supports local and universal naming conventions through three types of entity names: access names (used with the command language), descriptive names (e.g., from a NATO-wide data dictionary), and alternate names (e.g., aliases used for the convenience of one or more nations or one or more information system components). IRDS functions include adding, deleting, modifying, and copying entities and relationships, in addition to report writing.

IRDS Services Interface. The *IRDS Services Interface* gives an application program full access to all IRDS services, through whatever external call interface is provided by the language in which the program is written. The standard (ISO/IEC 10728) defines the semantics of this interface and specifies the language bindings for Pascal. IRDS facilities are formally defined with data structure diagrams and working set diagrams. Data structures are specified using SQL (without constraining the implementation approach). Services and formats for service data structures are specified, in part, using Pascal. Primary key, uniqueness, referential, and check constraints are included in each formal data specification and illustrated diagrammatically (using a "crow's feet" data modelling language). [Ref. SC21 N 8202 1993]

IRDS Standardization in ISO and ANSI. The IRDS is a data dictionary standard being developed in parallel by both ISO (JTC1 SC21/WG3) and ANSI (ANSI X3H4). The standard is based on the entity-relationship model and would be applicable to Database Language NDL and Database Language SQL.

ISO and ANSI differ in their approach to IRDS standardization as well as in the technical details. The communities have diverged over the issue of whether relationships are permitted to have attributes (ANSI) or not (ISO). The rationale for the simpler model (no attributes) is that it would fit more easily with SQL tables. The rationale for the ANSI position is that a model permitting attributes, while more complex and more cumbersome, would provide greater flexibility. Further, many existing products would be invalidated if no attributes were permitted for the relationships.

ANSI has developed three IRDS standards: (1) an IRDS with a human interface called a *Command Language and Panel Interface* (ANSI X3.138), (2) a software interface to the IRDS called the *IRDS Software Interface* (ANSI X3.185), and (3) *IRDS Export-Import File Format* (ANSI X3.195), which supports schema and metadata interchange among IRDS-compliant databases, among IRDS and CASE tools with repositories or dictionaries, and between IRDSs and application programs.

ANSI X3.138 was adopted by the US Government as FIPS-156, effective October 1989. An 18-month transition period to allow industry to produce and provide IRDS products during which users could use non-conforming products ended in March 1991. [Ref. APP 1991] While commercial products have been developed, their quality has not yet been determined because a conformance test suite is not yet available. Conformance tests are under development. [Ref. APP 1992] An upgrade to FIPS-156 is not expected until 1995. Most likely the revision will be influenced strongly by object-oriented data models as well as emerging repository and computer-assisted software engineering (CASE) technologies. [Ref. Price 1991]

ISO began a *Command Language and Panel Interface Standard* (DP 8800), but suspended the effort in 1987 when the ISO and ANSI efforts diverged. This project has since been cancelled. [Ref. SC21 N 8081 1993]

The *IRDS Services Interface* (ISO 10728) is comparable to ANSI *IRDS ATIS (Atherton Tools Integration Standard) Software Interface* (X3.185) in that it allows software (as opposed to humans) to access the IRDS; however, the technical details differ.

Revision of ISO 10728. ISO 10728, in combination with the *IRDS Framework* standard (ISO 10027), forms the basis for the first generation ISO IRDS standard (sometimes called IRDS1). Even though it only recently reached IS status, work has already begun on the second generation IRDS (IRDS2). A NWI for *IRDS Extensions* was introduced in October 1990 [SC21 N 5139]. Although the new work item proposal received the required number of approval votes to qualify for acceptance, several National Bodies submitted negative votes on the basis that a strong statement of requirements was lacking. Therefore, JTC1 did not make a formal project assignment [JTC1 N 1254]. SC21/WG3 responded with a revised scope of work, and the project was added to the JTC1 program of work in August 1991 [JTC1 N 1486] under the title *Extensions to the IRDS Services Interface.*

WD text for *Extensions to the IRDS Services Interface* is SC21 N 8208, September 1993. The IRDS group is making rapid progress on this project and is requesting permission to register it as a CD in July 1994 (it will be a second edition of ISO/IEC 10728). DIS is expected in 1995, and IS in 1996. [Ref. SC21 N 8123 1993] It will provide enhanced facilities in the following areas:

- IRDS class hierarchies, inheritance of data type and behavior, method registration, and specification and method invocation
- IRDS data types, including abstract data types and aggregations
- IRDS triggers
- IRDS services and data structures to support configuration management tools
- Further operations on working sets and their contents, including the combination of the contents of two or more working sets and possibly the division of the contents of a single working set into two or more working sets
- Extensions to cross-referencing
- Extensions to versioning
- Access to large numbers of IRD objects, possibly by means of access to multiple rows in one service invocation
- Work on level independent objects and services
- Improved handling of IRDS Content Modules, their inter-relationships and interdependencies
- Archiving
- Handling of extended character sets
- Access control.

IRDS Services Interface Extensions – Design Document [SC21/WG3 N 1283] is a standing document whose purpose is to record decisions made in connection with IRDS2. In addition, it contains general principles that will guide the work. [Ref. SC21/WG3 N 1283 1992]

Revision of ISO 10027. The *IRDS Framework* is also undergoing revision. The WD text is SC21 N 8204, September 1993. CD is expected in July 1994. The purpose of the revision [Ref. SC21/WG3 N 1406 1992] is to:

- Align the *IRDS Framework* with the *Reference Model of Data Management* (ISO 10032), which did not achieve CD status until after ISO 10027 was approved.
- Align the *IRDS Framework* with the ongoing work in the IRDS *Services Interface* (ISO 10728), SQL, RDA, and other related standards activities.

- Ensure that the *IRDS Framework* provides a sound basis for positioning standards needed to satisfy the user requirements as identified in the *ANSI IRDS Reference Model Draft Technical Report* [SC21/WG3 N 1208].

While the *IRDS Framework* revision brings together two major database standardization activities, it further complicates the alignment of the ANSI and ISO standards. Efforts on the part of ANSI X3H4 (IRDS) to seek reconciliation with ISO have not been successful [Ref. IST/21: 2499 1991]. WD status was achieved in July 1993 and CD status is expected in January 1994. DIS is expected in July 1995 and IS in July 1996. [Ref. SC21 N 8123 1993]

IRDS Overlap with PCTE. SC21 has noted the overlap between IRDS and the Portable Common Tool Environment (PCTE) (see Section 4.3.2.2) and has invited [SC21 N 7192] ECMA TC 33 to submit requirements concerning this overlap. SC21 submitted a request [SC21 N 8103] to JTC1 in June 1993 for a fast-track ballot of PCTE (DIS 13719, September 1993). Coordination with SC7 and SC22 is required. SC21 also requested informal talks before proceeding with a DIS on a second version of ISO/IEC 10728.

Other IRDS Projects. Other ISO projects related to IRDS include:

- *IRDS Design Support for SQL Applications*—CD text was expected in June 1992. However, in the absence of a WD, SC21 is reassessing the project. [Ref. SC21 N 7728 1993] A rapporteur meeting was held in January 1994, and a CD is expected in July 1994.
- *IRDS Export/Import*—CD text was expected in July 1993; however, this project has been cancelled and the work is being reorganized. [Ref. SC21 N 8081 1993] It is now being progressed as a three-part standard called *Data Management Export/Import Facilities* [SC21 N 8123 1993] (see Section 6.2.2.3).
- *IRDS Conceptual Schema*—December 1992 [SC21 N 7486] (working document).
- *Support for SQL1 with Integrity Enhancement*—working document scheduled for completion in 1993.
- *Guidelines for the Design of IRDS Content Modules*—A draft technical report that defines data structures to be supported by IRDS to meet the needs of specific area and provides an agreed approach to the development of IRDS content modules by various committees (e.g., SC7, SC21, TC184). At the same time, TC184 is moving slowly towards development of an IRDS content standard, and SC7 has a new work item proposal to develop models for methods. The proposal for a new work item in SC21 for the Guidelines document was accepted in April 1993, and a rapporteur meeting was held in January 1994. PDTR is expected in July 1994.

Semantic Unification Meta Model (SUMM). SC21/WG3 has also noted that there is a growing industry requirement for investigation of a unification meta model for the representation and manipulation of the data semantics managed by an information repository. In November 1991, WG3 posed a question [SC21 N 6251] on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM). The new question was approved and work began in June 1992. This requirement shares objectives with the conceptual schema and common data modelling facility issues (see Section 6.2.5). [Ref. SC21 N 6251 1991] WD text of the *SUMM: Technical Approach* [SC21 WG3 N 1360], Version 0.7-1, was published in October 1991.

A technical report on SUMM, *Technical Report on the Semantic Unification Meta-Model*, Volume 1, *Semantic Unification of Static Models*, October 1992, was prepared by the Dictionary/Methodology Committee of the Initial Graphics Exchange Specification (IGES)/Product Definition Exchange Specification (PDES) Organization (IPO) for ISO/TC184 SC4/WG3 [Ref.

SUMM 1992]. IPO develops US contributions to the *Standard for the Exchange of Product Model Data (STEP)* being developed by ISO/TC184 SC4/WG3. The report establishes a technical basis for addressing model integration problems that arise when the following three conditions, normally essential to integration, are not met: (1) using the same modelling language, (2) sharing a common culture of experience and background, and (3) having a single agreed methodology to guide the work. SUMM is a model of the semantic structure of formal languages and of the semantic similarities between those languages. The original work on SUMM was motivated by the need to accurately translate an information model (often called a data model) written in one formal language into an equivalent model stated in a different language, based upon common underlying principles. An example would be the conversion of an model defined by Nijssen Information Analysis Method (NIAM) into Integrated Computer-Aided Manufacturing (ICAM) Definition Language Type 1 Extended (IDEF1X). [Ref. SC21/WG3 N 1644 1993]

Remote IRDS Access. WG3 has also noted a growing industry need for interoperability. In the IRDS context, CASE tools on workstations need to access dictionaries on servers. Therefore, WG3 recommended that SC21 ask JTC1 to initiate a ballot for the registration of a question (Q3/009) on the Approach to Remote IRDS Access. [Ref. SC21 N 6253 1991] JTC1 authorized work to begin in June 1992. The question has eight parts, reproduced below with the draft answers in italics [Ref. SC21 N 7181 1992]:

1. What are the requirements for the access by a client application in one real system to IRDS Services, as defined in ISO 10728 *IRDS Services Interface*, provided by a server in a different real system? *The requirement is for applications such as CASE tools to be able to use IRDS services to access IRDS data in a local IRDS (in the same real system), in a work group IRDS (in another autonomous real system), or in a corporate IRDS (in another real system to which the local system is to some extent subservient).*
2. What facilities are required to be standardized? *A mechanism for communicating IRDS service requests and responses between two real systems.*
3. In what way or ways should ISO standardize access by a client application in one real system to IRDS Services provided by a server in a different real system? *At least by an IRDS Specialization of Remote Database Access, based on the SQL Specialization of RDA (ISO 9579-2).*
4. Should the proposed Standard be consistent with:
   a. ISO/IEC 10027: *IRDS Framework*
   b. ISO 9579-1: *Remote Database Access - Generic*
   c. ISO 9579-2: *Remote Database Access - SQL Specialization*
   d. ISO 10728: *IRDS Services Interface*

   Yes, with all of these as far as possible, though the differences between IRDS and SQL will necessitate some differences from ISO 9579-2.
5. Should the proposed standard define a specialization of the generic RDA protocol or should it provide the required facilities by some other means? *To minimize the work involved while meeting the identified requirements, the standard should build on existing work by defining a specialization of the Generic RDA protocol, based where possible on the existing SQL Specialization of RDA.*
6. Should this specialization support the access to IRD Definition level and IRD level data by means of the invocation, by a client in one real system, of the services specified by ISO 10728 *IRDS Services Interface*, provided by a server at a different real system? *Yes.*

7. **Should the notations and mechanisms used to prescribe the Remote IRDS Services protocol be those used in ISO 9579-1 (*Remote Database Access - Generic*)?** *Yes.*
8. **Should the design of the protocol be restricted to being as close as possible to that defined in the SQL specialization of RDA specified in DIS 9579-2?** *Not restricted, although the SQL specialization of RDA is likely to form the starting point.*

Although a NWI request for *Remote IRDS Access* [SC21 WG3 N 1384] had been proposed, it was dropped until consensus on the answer to the above questions could be obtained.

An IRDS Content Module is a set of definitions prepared for use with an IRDS. Content modules may be defined by methods developers as a precursor to building CASE tools to support their methods, by language developers requiring IRDS support for a programming language, by DBMS developers wishing IRDS support for their DBMS, and by many other classes of potential IRDS users. The ISO IRDS Rapporteur Group has drafted a standing document on *Guidelines for the Design of IRDS Content Modules* [Ref. SC21/WG3 N 1272 1991], and the project has been accepted into the JTC1 program of work. [Ref. SC21 N 7742 1993]

Experts representing *CASE Data Interchange Format (CDIF)*, IEEE P1175 (*Reference Model for Computing System Tool Interconnections*), and *Product Definition Exchange Specification (PDES)* are working to develop an *IRDS Content Module Standard for Software Engineering* to support the data flow modelling subject area. [Ref. SC21 WG3 N 1279 1991] In June 1992, the SC21 Plenary accepted a new work item proposal for a Technical Report [SC21 N 7178] entitled *Guidelines for the Design of IRDS Content Modules* for ballot by SC21. The target dates were WD in June 1993, CD in June 1994, DIS in June 1995, and IS in June 1996. [Ref. SC21 N 7178 1992]

IRDS Export/Import File Format, became an ANSI standard (X3.195-1991) in 1991. *Support for Naming Convention Validation (NCV)* was approved in 1992 as X3/TR-11. Several other ANSI IRDS efforts are nearing US public review status while one has been completed and another new work area has been initiated [Ref. Winkler 1991]:

- *Technical Report on the IRDS Reference Model.* This report will explain the relationship of the IRDS within the information environment of an enterprise.
- *Technical Report on Requirements for an IRDS in a Distributed Heterogeneous Environment.* This document, under development by X3H4.5, is progressing slowly.
- *Technical Report on Integration of IRDS Schema.* This report is currently inactive. Instead, X3H4.6 is working on a *Technical Report on Model Unification for Data Repositories,* which will address the same problem but at a different level. The technical report will address the needs of IRDS users to translate, integrate, reference, and/or use differing models or representations of enterprise information and behavior at various levels of complexity and abstraction. It will establish a framework for the analysis of models; analyze models; define the IRDS neutral unification model and its representation; reconstruct models using the unification model; develop an IRDS meta-schema; develop IRDS requirements; develop IRDS conceptual model architecture guidelines; and develop a test case. The original target date was January 1993.
- *Standard on Export/Import Extensions.* ANSI X3H4 cannot progress this standard until the *Technical Report on Model Unification for Data Repositories* is complete.
- *Technical Report for IRDS Administration and Control* was expected in 1993.

ANSI X3 recently announced a development project for IRDS *Extensions to Support CASE Environment for Information Interchange.* This standard would define an IRDS, based on ANSI X3.138-1988, capable of supporting the full range of IRDS applications. In particular, it

would be capable of acting as the IRD in a traditional data processing environment and capable of providing the stable store necessary to support an integrated CASE environment. The standard would include both the semantics of the IRDS and a software interface suitable to the needs of active CASE and Dictionary tools. The development has been assigned to Technical Committee ANSI X3H4.2. [Ref. CSI 1990]

IRDS Services Architecture Technical Report, January 1993 [Ref. IRDS 1993], is an ANSI X3H4.1 working paper that will become Part Five of the full set of documents titled "Framework for the Evolution of IRDS Standards." Taken collectively, these documents are intended to provide a picture of the full strategic scope of IRDS systems as it is currently understood. The structure of the Framework for the Evolution of IRDS Standards is outlined in Table 6.

Table 6. Structure of the Framework for the Evolution of IRDS Standards

Part	Title	Purpose
Part One	IRDS Strategy	Define IRDS standardization strategy
Part Two	IRDS Program Plan	Detail the program of work with deliverables, schedules and responsibility for task execution
Part Three	IRDS Operational Concepts	Illustrate scenarios of IRDS use within an enterprise
Part Four	IRDS Context Reference Model	Establish IRDS universe of discourse within the context of the enterprise's information system environment
Part Five	IRDS Services Architecture	Define architecture for organizing IRDS services and interface mechanisms
Part Six	IRDS Requirements	Specify usage and system requirements to guide development of IRDS standards
Part Seven	IRDS Conceptual Schema	Specify discipline for defining the semantics of IRDS contents
Part Eight	Evolving the IRDS Information Model	Specify the press for evolving the integrating application content modules
Part Nine	IRDS Administration	Document functions and procedures needed to administer an IRDS environment
Part Ten	IRDS Inter-Relationships	Explain harmonization strategy and the relationships of IRDS models, architectures and standards to related efforts
Part Eleven	Glossary	Present specialized definitions for IRDS terminology

Source: [Ref. IRDS 1993]

6.2.5 Conceptual Data Modelling Facility Standards

6.2.5.1 Conceptual Schema

SC21/WG3 has identified five different uses of the term "conceptual schema." The following identifies the five uses and provides WG3 comments on those uses [Ref. SC21 N 4195 1990]:

- The results of an analysis of the data and possibly the processes perceivable in some real-world situation.
  - There is considerable disparity among the data analysis techniques used in various parts of the world. Some are being energetically promoted by minority groups.
  - There are rapid developments in CASE.
  - Attempts to standardize on any one technique may be premature. Such efforts should await availability of the Reference Model on Information Systems Engineering being developed by SC7/WG4.
  - Work on a conceptual data modelling facility should be considered as content of an IRDS and be conducted in accordance with the IRDS Framework (ISO 10027).

- A repository of "metadata" in which it is possible to specify declaratively 100% of the semantics of the data in a computerized information system (the 100% principle of TR 9007). The "100% principle" now adopted by ISO [Ref. SC21 N 197 1982; SC21 N 236 1985] says:

  > All relevant static and dynamic rules, law, etc., about the universe of discourse should be described in the conceptual schema. The information system cannot be held responsible for enforcing those rules described elsewhere, particularly those described in user procedures.

  - The 100% principle has had major influence on SC21/WG3 work in the development of SQL. The SQL draft proposal being progressed contains language specifications that make it possible to specify declaratively a very large percentage of the constraints on the data that a database designer is ever likely to want to define.
  - While SQL is never promoted as a means of defining a conceptual schema, it is, in this very important respect, superior to many of the approaches developed especially for the purpose.
- A data definition that has the property of being independent of its representation in storage.
  - Some standards committees have adopted the term to refer to some kind of representation of the data definition that is above the level of stored representations.
  - SQL is a language that enables the preparation of a storage independent definition of data.
- A data definition that is common to the collections of data at two separate sites, such that it can be used as a common frame of reference when exporting data from one site and importing it at another site.
  - In EDI, one needs a definition of data to be interchanged that is common to all sites involved in a set of interchanges.
  - Much of the EDI work has been concerned with the specification of standard formats for an industry area, such as banking or travel. As EDI tends to adopt a more generalized approach to standardization, the need for a common definition facility becomes apparent.
- A data modelling facility (see ISO 10032, the *Reference Model on Data Management)* that is different from and therefore "neutral" with respect to broadly similar data modelling facilities used in commercially available database management systems.
  - Data modelling facilities are also called data models; merits of various approaches are controversial topics.
  - Another "neutral" approach would lead to confusion, is not required, and is not recommended by WG3.

6.2.5.2 Conceptual Schema Standardization

Work in the area of conceptual schema in ISO dates back to the early 1980s. In 1982, TC97/SC5 first published what is now TR 9007, *Concepts and Terminology for the Conceptual Schema and the Information Base*. This report was followed in 1985 by the *Assessment Guidelines for Conceptual Schema Language Proposals*.

SC21 held a workshop on conceptual schema and its relationship to the Conceptual Data Modeling Facility in the Netherlands in November 1990. A subsequent workshop was held in Anaheim, California, in January 1991 where papers on some 18 different modelling methods were

presented. Two of the approaches presented included the ANSI IRDS approach and the ANSI X3.T2 Registering of Conceptual Schemas approach. [Ref. Perez 1991]

ANSI has proposed that a new question be established in SC21 to determine the use, scope, and purpose of one or more standards for conceptual schema. The goal would be to address the need for models of a "universe of discourse (UOD)." Such models are needed to clarify in a formal way the notion of a particular universe of discourse to which a standard applies (e.g., for Directory schema) and to facilitate the specification of a common universe of discourse for information exchange (e.g., for *Application Layer Structure,* ISO 9545). [Ref. SC21 N 4511 1990] Actions of such an international standards activity might include: (1) developing and maintaining a list of approved answers and comments on issues related the topic of conceptual schemas; (2) registration; and (3) developing and maintaining one or more standards for specifying inter-application information requirements, semantics, concepts, and terminology for open applications. [Ref. SC21 N 5851 1991]

The United States is developing a national standard for conceptual schema based on the Integrated Computer-Aided Manufacturing (ICAM) Definition (IDEF) graphical methods for defining the functions, data structures, and dynamics of manufacturing businesses, the result of US Air Force studies in the late 1970s. The data modelling language IDEF1X, developed by Hughes Aircraft and the D. Appleton Company, provides an entity-attribute-relationship conceptual schema for specifying data requirements and improving the quality of database designs. [Ref. Bruce 1992]

A US standard has been issued: FIPS 184, *Integration Definition for Information Modeling (IDEF1X),* National Institute for Science and Technology, 1993. It has an effective date of 30 June 1994.

As noted in Section 6.3.1 below, entity-attribute-relationship data models are now being required in the US DoD for the basis of future data standardization. IDEF1X has been adopted as the standard for presenting data models. IDEF1X was used to develop the *Army Data Model* (which defines data at the Army Staff level), the *Battlefield Generic Hub* [Ref. ATCCIS WP 5-2 1992] and the *Fire Support Data Model* [Ref. ATCCIS WP 5-2B 1992] (IDEF1X data models have also been developed in ATCCIS for engineer, personnel, and communications-electronics). The Data Management Directorate of the US Army Information Systems Engineering Command developed the *Army Data Model* and is actively working on others. These and 25 additional projects have been identified [Ref. DISA/CIM 1992] by DISA/CIM in the area of business process improvement, all of which will eventually require data modelling.

ANSI X3T2 Data Interchange Committee has a domestic standardization project entitled, "Conceptual Schema Specification for Data Interchange." The purpose of the project is to define a model, technique, and language for specifying formal and informal conceptual schemas. The scope of the project is to standardize a declarative technique for specifying and structuring information semantics in a form independent of, and compatible with, three ISO information standardization environments: (1) communications, (2) processing and display, and (3) databases and storage. The base standard for this standard will be TR 9007, July 1987.

In April 1993, X3T2 issued a request for early review and comment on this project. Specifically, it has identified a technique and language that appears to meet a significant portion of the functional requirements for the proposed standard. This is the *Knowledge Interchange Format (KIF)* [SC21/WG3 N 1645] by the Interlingua Working Group of the DARPA Knowledge Sharing Effort. The document [Ref. Genesereth 1992] is in Version 3.0. [Ref. X3T2/93-048

1993] KIF is a formal language for the interchange of knowledge among disparate computer programs (e.g., written by different programmers at different times in different languages). The specification includes declarative semantics with expression of arbitrary sentences in predicate calculus and representation of knowledge *about* the representation of knowledge. [Ref. SC21/WG3 N 1645 1993]

6.2.5.3 Conceptual Data Modelling Facility Standardization

Japan proposed a new work item in SC21/WG3 for a conceptual data modelling facility [SC21 N 4280, February 1990]. The proposed standard would specify the facility to describe an application data model and the representation method of the result of the description of an application data model. A Special Meeting on Conceptual Schema and Common Data Modelling Facilities was held in Renesse, Holland, March 1992. It addressed the following issues [Ref. SC21 N 6449 1991]:

- Requirements of various international standards groups using the concepts and terminology of conceptual schemata
- Interfaces and mechanisms employed to model, specify, use, and relate conceptual schemas in these activities
- Identification of the standardization groups now using, or planning to use, conceptual schema techniques or common data modelling facilities
- Relation of the requirements and uses identified above
- Identification of activities for the standardization of conceptual schema techniques or common data modelling facilities and interfaces to them being undertaken by National Bodies or by other standards organizations
- Planning and organization of future work on conceptual schemas
- Consideration of whether and how a conceptual schema can be stored and interchanged using standard database languages
- Addressing the short-term considerations of coordination amongst the various standardization groups within JTC1
- Relationship of proposals made to existing standardization activities in the area of reference models and frameworks.

The output of the meeting consisted of recommendations for six new JTC1 projects [Ref. SC21 N 6945 1992]:

- A question on "the use of Standardized Conceptual Schema and Data Modelling Facilities in the definition of JTC1 and other ISO standards"
- Development of a *Standard Lexicon of Conceptual Schema Concepts*
- Preparation of a technical report entitled *A Framework for Model Comparison Transformation and Integration*
- Development of a standard for a *Conceptual Schema Facility*
- Preparation of a technical report entitled *A Case Study on the Harmonization of Standards Models in the Areas of Information Technology and IT Application*
- Development of a standard for *An Architecture for Supporting Conceptual Schema Facilities.*

Recognizing the severity of the problem, the SC21 Secretariat called a tutorial session in May 1992, during its Plenary to discuss data modelling facilities, including major results from the Renesse workshop. SC21 requested that WG3, WG4, WG6, and WG7 discuss and do

preliminary work on the following issues at their meetings in Ottawa in May 1992 [Ref. SC21 N 6614 1991]:

- Relationship between WG3 database standards and data modelling facilities relating to the Management Information Base of WG4 OSI Management standards
- Relationship between WG3 database standards and the data modelling facilities supported by WG4 Directory Services standards
- Relationship between the data modelling support facilities of WG3 and the information viewpoint concerns in the Reference Model of ODP
- Relationship between the Remote Database Access server format supported by the WG3 work and the ASN.1 extensions being developed by WG6 (e.g., support of tabular data); and the relationship between the ASN.1 and its extensions and the facilities for the description for data definition within an SQL database.

Also at its Plenary in May 1992, SC21 formed a Special Working Group (SWG) for a Study Period on the topic of Modelling Facilities (MF) applying the procedures for the preparation of large new work item proposals. The SWG-MF considered three topics [Ref. SC21 N 7208 1992; DRA 1994]:

- Use of a standard data modelling facility in defining standards
- Requirement for a standard conceptual schema facility
- Inter-relationships between such a conceptual schema facility and the use of a standard.

One product of the SWG-MF is the *Proposed Working Draft for Base Document for Conceptual Schema Modelling Facilities*, October 1992 [SC21/WG3 N 1646].

An SWG-MF meeting on modelling facilities held in Namur, Belgium in December 1992 yielded papers on the following topics:

- Modeling facilities proposal for a new program of work [SC21 N 7546]
- Interrelationships between a conceptual schema modelling facility (CSMF) and a data modelling facility (DMF) [SC21 N 7545]
- Requirements for standard modelling facilities [SC21 N 7544]
- Use of standard modelling facilities in the definition of JTC1 and other ISO standards [SC21 N 7543].

The final report of the SWG-MF [SC21 N 8056] emphasized the last topic, using standard modelling facilities in the preparation of standards. The SWG-MF proposed the following definitions [Ref. SC21 N 7542 1993]:

- Data Modeling Facility (DMF)—a system (possibly incorporating methods, languages, software tools, etc.) that enables and supports some or all of the activities surrounding a data model, that is, its creation, update, management, linkage with external knowledge representations, and all relevant services involved in its life cycle.
- Conceptual Schema Modeling Facility (CSMF)—a system that enables and supports the activities surrounding a conceptual schema. Since a conceptual schema subsumes a data model, any CSMF must contain or interoperate with one or several DMFs.

The SWG-MF identified the following standards and standards projects as already making use of a DMF: ODA (ISO 8613), *IRDS Services Interface* (ISO/IEC 10728), *Design Support for SQL92 Applications* (SC21/WG3), *Database Language SQL* (ISO/IEC 9075:1992), *Information Framework* (ISO 9594-2), *Selected Attribute Type* (ISO 9594-6), *Selected Object Classes* (ISO 9594-7), *Management Information Model* (ISO/IEC 10165-1), *Definition of Management Information* (ISO/IEC 10165-2), *Application Layer Structure* (ISO/IEC 9545), *Data Flow*

Diagrams (SC7/WG1), *State Transition Diagrams* (SC7/WG1), *Product Data Exchange - EXPRESS* (ISO/IEC 10303-11), *CASE Interchange Metamodel* (EIA/CDIF), and *Reference Model for Computer System Tools* (IEEE P1175). Projects likely to make use of a DMF in the future are Conceptual Schema for Open EDI (JTC1/WG3), Data Element Coordination Group (TAG7/DCG-NIAM DMF), Guidelines for Design of IRDS Content Modules (SC21/WG3), ODP SC21/WG7), Data Elements and Exchange Formats (TC46/SC3), and Data Elements (TC46/SC4/WG7). [Ref. SC21 N 8057 1993]

SC21 approved a new work item proposal on *Conceptual Schema Modeling Facility*, June 1993 [SC21 N 8060]. This work would standardize a CSMF as the basis for specifying concepts and terms about one or more subject areas (e.g., areas for standardization)—the CSMF would assist in building an abstract model of the subject area. A CSMF is viewed as an urgent need to provide a consistent facility to be used in preparing other standards. At its plenary in June 1993, SC21 dissolved the SWG-MF and established a rapporteur group under WG3 to progress contributions on CSMF on an interim basis based on a draft contribution [SC21 N 8086]. Work by the CSMF Rapporteur Group was directed to be on use of modelling facilities in standards preparation. The focus of work on data modelling was directed to be limited to identifying requirements for the use of a DMF in the preparation of standards and reviewing existing DMF standards for applicability rather than creating a new DMF standard. [Ref. SC21 N 8081 1993; DRA 1994] The CSMF Rapporteur Group met in January 1994 to define concepts, terms, principles, functional capabilities, and framework for standard Cosmos [Ref. SC21 N 8282 1993]. The next meeting is planned for July 1994 [Ref. SC21 N 8127 1993] The following are recommended standards and related documents for CSMF work [Ref. JTC1 N 2775 1993]:

- *A Data Modelling Facility: JDMF/MODEL-1992* [SC21 N 8305 1993] (English translation of a document from the Japanese Standards Association)—describes data construction rules for an application data model (defined to be a model of an object world from a data point of view) shared for many purposes and a representation method of describing such a data model. Data construction rules are characterized as consisting of data structures describing relationships among data and integrity constraints to be satisfied among data. The facility defined by this document is an object-oriented data modelling facility in the sense that its basic component is an object embodying data about itself and operations applicable to it.
- *Conceptual Schema Specification for Data Interchange*, ANSI/X3 689-D
- *Information Resource Dictionary System Normative Schema*, ANSI X3 988-D
- ISO TR 9007, *Concepts and Terminology for Conceptual Schema and Information Base*
- *Assessment Guidelines for Conceptual Schema Language Proposals* [SC21/WG5 N 236]
- ISO/IEC 10303-11, *Standard for the Exchange of Product Model Data (STEP)*, Part 11: *EXPRESS (Language Reference Model).*

6.2.5.4 Object-Oriented Database Support

In 1989, the ANSI X3 Standards and Planning Requirements Committee (SPARC) Database Systems Study Group organized the Object-Oriented Database Task Group (OODBTG) to gather information on object database management systems and to recommend standards needed in this area. Their final report, issued in October 1991, contains the following [Ref. ANSI 1991]:

- Recommendations for standards in object data management
- Reference model for object data management

- Glossary of object data management terms
- Report on a survey of object data management systems
- Report on workshops on object data management standardization.

In June 1991, SC21/WG3 recommended that SQL support for objects continue to be developed via the SQL3 specification and that the Reference Model rapporteur group consider other requirements, as appropriate beyond SQL. [Ref. Gallagher 1991] WG3 posed a question (Q3/001) on support for object orientation in database. In its answer to Q3/001, WG3 stated that for the purpose of WG3, the question is resolved by the SQL-3 related work being done in support of the object paradigm.

In early 1992, ANSI X3 announced the formation of a new technical committee, X3H7, Object Information Management (OIM). The object paradigm is increasingly used as a basis for interoperability in the areas of object data management, object programming languages, object networking, object analysis and design, and object user interfaces. X3H7 will develop a reference model technical report the scope of which will include the following [Ref. X3 1992]:

- An interoperable object model
- Object data management services
- External representations of object model schema and data
- Object class libraries
- Object languages
- Object communication and distribution
- Object design and methodologies.

The final standard from ANSI X3H7 (Object Information Management committee) will be the tool for providing connectivity between many different standards. The committee is providing a framework for harmonizing the different object models, object interaction designs, object database, and distributed system/object standards. The core of the initial standard is a "Features Matrix" that provides a comparison of the object models of existing object database models. The standard is being developed with the coordination of several other ANSI committees and the Object Management Group (OMG). It is expected to be available for coordination by 1994. [Ref. CFS 1993c]

6.2.5.5 Full Text Manipulation in Structured Data

SC21/WG3 is including in its work on SQL standardizing support for full text manipulation in combination with the management of structured data using SQL. SQL:1992 supports storage of a collection of text as a single data value, but is not capable of the complex requirements for full text manipulation. [Ref. SC21 N 5141 1990] A special WG3 ad hoc meeting on the question of Free-Text Database (Q3/002) recommended that full text be pursued as part of a broader, new project on SQL/Multimedia (see Section 6.2.2.2). [Ref. SC21 WG3 N 1430 1992]

6.2.6 Transaction Processing

A transaction is a logical set of operations characterized by the four properties: atomicity, consistency, isolation, and durability (ACID). The atomicity property means that, to an outside observer, either all of the operations are completed or none of them is executed. The consistency property means that the operations are performed correctly with respect to the application semantics. The isolation property means that any partial results of the operations composing the

atomic action are not accessible before the completion of the atomic action. Finally, the durability property means that the action must endure a communication or an application failure.

The OSI Transaction Processing (TP) standard (ISO/IEC 10026) provides an infrastructure to support distributed transaction processing which may span across one or more open systems. It provides mechanisms to ensure the ACID properties of a distributed transaction and a transaction processing environment involving a number of application associations. TP concepts, standards, and profiles are described with other network services in Section 9.11.9.

6.2.7 Other Database Service Standards

CODASYL data management standards are the responsibility of the CODASYL Systems Committee. A report on distribution alternatives and generic architectures for distributed database systems was produced by this committee in 1980. [Ref. CODASYL 1980] One of the two standard ISO data management languages (NDL) is based on CODASYL concepts.

In 1985, ECMA[31] issued a final draft report [Ref. ECMA 1985] for remote database access service and protocol.

ANSI standards for database architectures are produced by the Database Architecture Framework Task Group (DAFTG) through the Standards and Planning Requirements Committee (SPARC). A draft report [Ref. DAFTG 1982] from the DAFTG in 1982 provided a framework to support distributed databases, multiple data models, and data dictionaries. One concept, the ASN.1, has been specified [ISO 8824 and 8825].

ITU-TS does not provide standards for data management. The US Government Open Systems Interconnection Profile (GOSIP, see Section 16.1.3.1) does not address standards for data management. [Ref. GOSIP 1988]

6.3 Standards for Data Management

6.3.1 Data Element Standardization

The following standard related to data management has been developed for the US DoD:

- DoD 8320.1-M-1, *DoD Data Element Standardization Procedures,* ASD(C3I), January 1993, UNCLASSIFIED.

Others are being developed:

- DoD Instruction 8020.1, *Functional Process Improvement Program,* Draft, 1 October 1992, ASD(C3I), UNCLASSIFIED
- DoD 8020.1-M, *Functional Process Improvement (Functional Management Process for Implementing the Information Management Program of the Department of Defense),* Draft, 5 August 1992, UNCLASSIFIED
- DoD 8320.1, *DoD Data Administration,* ASD(C3I), 26 September 1992, UNCLASSIFIED
- DoD 8320.1-M-X, *DoD Data Model Development, Approval, and Maintenance Procedures,* Draft, May 1993, UNCLASSIFIED
- *The DoD Enterprise Model,* Volume I, *Strategic Activity and Data Models,* January 1994.

---

31 ECMA full membership is open only to companies who develop, manufacture, and sell computers in Europe. The restricted membership makes full consensus among participants in standards-making easier and quicker to reach than in ISO.

The US DoD has mandated that "DoD operations shall be executed through integrated and standard Department-wide process, data definitions, and information systems in support of joint warfighting and peacetime missions" [Ref. DoD Instruction 8020.1 1992]. The DoD has developed standards, many still in draft form, to implement centralized data administration, including DoD 8320.1, 8320.1-M, and 8320.1-M-1. Such data administration seeks data standardization that supports the following:

- Providing clear, concise, consistent, unambiguous, easily accessible data DoD-wide
- Minimizing the cost and time required to transform, translate, or research differently described, but otherwise identical, data
- Supporting data sharing and interoperability among information systems throughout the DoD
- Providing uniform description and representation of data.

Data element standardization will be governed by DoD 8320.1-M-1. As atomic single-concept specifications, data elements will be defined and classified to represent the attributes of data entities identified in entity-attribute-relationship data models. Their definitions will be based on data entities and their associated attributes established in a DoD-wide data model. Single-concept data elements will be specified to promote shareability and data independence for applications.

ISO has issued a standard (DIS 7826) on the representation of data elements. This draft proposal sets out standard procedures for the identification and representation of existing and new coding systems, without providing any guidance on specific coding systems. It also specifies a technique for interchange of coded representations and the requirements for the administration of International Coding System Identifiers (ICSIs). This will permit the use of more than one coding system, reduce the possibility of ambiguity, reduce the need for human intervention, and diminish the time required to negotiate interchange of coded representation agreements. DIS 7826 identifies three types of data element attributes: administrative, relational, and representative.

The US Army has published an Army Regulation (AR 25-9) [Ref. DISC4 1988] to prescribe policies, responsibilities, and concept of operation for the management of data used in manual and automated information systems throughout the US Army. This document has been coordinated with ISO, ANSI, and the NIST, as well as with the US Joint Chiefs of Staff, to ensure alignment in the area of a data element naming convention. The US Army plans to maintain a Service-wide data encyclopedia of information about all data elements that have gone through a standardization process and are designated as Army standard elements. AR 25-9 has been used for initial work on data element standardization for CIM. Additional information on AR 25-9 is provided in ATCCIS WP 7L. [Ref. WP7L 1989]

Substantial work has been done cooperatively by ISO JTC1/SC14 and ANSI X3L8 during the last 5 years. This work has resulted in an X3L8 document entitled *Coordination of Data Elements*, which was accepted by SC14 as document SC 14 N 492. It is DIS 11179, which has six parts. Two other ISO Technical Reports are in progress:

- DTR 7352, *Guidelines for Grouping of Data Elements in the Context of Data Interchange*
- PDTR 9789, *Guidelines for Data Interchange - Coding Methods and Principles*

The objective is for application areas to interchange data among themselves predicated on shared generic concepts that would be documented in a Data Element Concept Taxonomy. [Ref.

Kenworthy 1991] The general approach to the structure of data recommended in AR 25-9 and ATCCIS WP 7L was derived from discussions with ISO JTC1/SC14 and ANSI X3L8.

6.3.2 NATO Policy and Issues for Data Management

6.3.2.1 NACISC Policy on Data Management

In June 1993, the NACISC promulgated a data management policy for NATO [Ref. NATO 1993a]. It provides a NATO policy for data management throughout the NATO Interconnected Information System (NIIS). It specifies the requirements and identifies the (1) elements of data management subject to NATO policy, procedures, and standardization and (2) the activities required. It further identifies the extent of standardization required for different elements of data management. The scope of the policy is to fulfill the requirements to: identify the responsibilities, organizations, and roles for data management within NATO; define data management and its elements and the extent to which they are subject to a NATO policy; state the principles, rules, standards, and procedures for the planning and implementation of data management; and identify the implications/overheads of successfully implementing data management. Table 7 provides excerpts from the policy document.

6.3.2.2 ADSIA Recommendations on Data Management

In April 1986, ADSIA revised a working paper [Ref. ADSIA 1987] on the need for standardization of data management. The following actions were recommended:

- NATO Communications and Information Systems Agency (NACISA) to identify and collect the requirements for database management systems and for standardization of database schemes, file transfers, database information exchange, and configuration management procedures
- Subsequently, the Information Systems Working Group (ISWG) to develop a NATO policy on data management and on the use of database management systems in NATO information systems
- ADSIA to coordinate the development of technical and procedural standards for databases
- ADSIA to develop the procedural standards for database information exchange
- TSGCE SG9 to develop technical standards for database schemes and file transfer
- NACISA to control the implementation of the developed standards and NATO policy paper to ensure the interoperability of command and control systems within the NATO information system.

6.3.2.3 NATO Interoperability Management Plan (NIMP)

Many aspects of data management are procedural in nature and will be controlled by procedural and not technical standards. Several of these standards are also identified below. The NATO Interoperability Management Plan (NIMP) [Ref. NIMP 1988] specifically identifies standards and rules for representing data as information procedural standards and assigns the responsibility for these standards to the Allied Data Systems Interoperability Agency (ADSIA). To emphasize the role of data management in achieving interoperability, the NIMP states:

> *In order for the information exchange to be effective, it is necessary that the meaning and relationships associated with that information [received from other facilities] is common and preserved, irrespective of the interoperability service and transmission media. A single common definition for all operational information throughout NATO is needed to achieve this goal.*

Table 7. NATO Data Management Policy

- Efficient interoperability in the NATO Interconnected Information System (NIIS) requires consistency and integrity of data throughout these systems. This in turn requires the application of NATO-wide standards and procedures for data management in this situation. The use of invalid data or the incorrect interpretation of data by other information systems can be disastrous for any type of operations. Each form of data exchange is worthless unless the meaning of data is understood unambiguously on both sides. Furthermore, if data is represented in different ways, translation will be required, which in turn hinders effective communication. Therefore, data management with its inter-system functions has to be planned and implemented to support the interoperation of systems by *preserving meaning and relationship in the exchange of data.* (Emphasis added.)
- Data management is defined as the planning for, organization, and control of data utilizing rules, procedures, people, methods, and tools to identify, define, and represent the meaning and relationship of data and to ensure its availability, quality, integrity, and security. Data management addresses all functions needed for the definition, storage, retrieval, manipulation, protection, and distribution of data.
- Data management functions support the operation of a stand-alone as well as distributed systems and the information exchange among systems. These functions are
  - Data security—the protection of data from either accidental or unauthorized intentional modification, destruction, or disclosure.
  - Data definition—the operational meaning of data, relationship with other data, data labelling (including classification), and representation of the data in information systems and in the information exchange with other systems.
  - Data manipulation—the capability to perform data operations in local and remote databases; typical data operations are to retrieve, store, append, update, and delete data.
  - Data distribution—the capability to disseminate data among databases and systems, whose pattern of distribution is dependent upon the operational need to provide information to interoperating information systems.
  - Data availability—the capability to enable the users to access their data from predetermined locations, within agreed response times, and must expect recovery with predesignated times following preplanned, accidental, or other loss of service. This implies five subfunctions:
    - Data monitoring—observes the values of elements in the database for analysis
    - Data transaction monitoring—logs data transactions and maintains statistics with a view to analyzing and verifying he performance of data management
    - Data backup—is concerned with the provisions and procedures to provide the data for recovering after a system failure in any form to ensure continuous operation with correct data
    - Data recovery—performs all the actions necessary to allow recovery of data after system failures
    - Data audit trails—deals with the provisions, procedures, and data for tracing the transactions that have affected the data.
- Data management functions are supported by the following tools:
  - Data model—an abstract representation (description) of real world items that represents structure (organization) of data and may exist in graphical format (e.g., entity-relation diagram) and a formal specification (schema) described by use of a data definition language, and corresponding entries in a data dictionary.
  - Data dictionary—a database that contains metadata (data about data) and rules that deal with the use and structure of data objects of a certain set of applications.
  - Database management system (DBMS)—a computer-based system for defining, creating, manipulating, controlling, managing, and using databases. A DBMS should have at least the following functions: support data definition, perform data manipulation, support data security, maintain data integrity, perform data monitoring, manage data distribution, support data recovery, and perform data system monitoring.

Source: *NATO Data Management Policy,* June 1993 [NACISC 1993a].

6.3.2.4 SHAPE Policy

The purpose of data management in NATO is to provide methods to ensure data availability, security, integrity, quality, and interoperability, and to provide data sharing. The *ACE Manual (AM) on Data Management,* AM 96-1-4 [Ref. SHAPE 1988], defines data as representing the elementary facts, descriptions, and qualifications about things of interest to some headquarters, unit activity, or enterprise. It further defines the role of a data dictionary as an automated tool that provides a centralized library of metadata covering all aspects of all types and structures of data residing in databases, file systems, and manual systems within an organization. AM 96-1-4 further asserts that:

- Evolution towards an ACE ACCIS will only succeed from the data management point of view by ensuring that the standardization of data definitions, the control of the data,

and the maintenance of its overall integrity are systematically established on a command or site basis.

- The fundamental key to data management is the early definition and identification of data elements and, later, data fields. The definition and corresponding name should be clear, accurate, and meaningful, but reference should be given to connotation, which relates to the interpretation that bears upon the specific context of usage of data.

6.3.2.5 STC Work

In 1975, Shape Technical Centre (STC) published a Technical Memorandum (TM) (TM-776) on data management standardization for the ACE ACCIS [Ref. SHAPE 1985]. TM-776 recommends standardization of the architecture, functionality, and structure of the Data Management Subsystem (DMS) of the ACE ACCIS. These areas of standardization include data management methodologies and the tools used to design, build, and maintain the ACE ACCIS databases. TM-776 accomplished the following:

- Identified the requirement that the DMS at each ACE ACCIS node must agree on the semantics and syntax of the information exchange.
- Recommended that there be a standard ACE data definition or conceptual schema, where a schema defines all application object types, including their attributes, relationships, and static constraints, and where a database is an instance of a schema.
- Stated that a data classification method must be used that is based on the principle of sorting data according to the type of information provided by their values, independent of their use in particular databases, messages, or applications.
- Identified the need for a methodology for formal definition of data elements based on standardized terminology, including the use of naming conventions:
    - A data element is defined as a basic unit of data that has a name, a definition, and a set of values for representing particular facts. A data element and its definition should not include any application or usage information.
    - A method is needed for analyzing, defining, and controlling data elements. This method should have three components: a type classification of data elements, syntax rules for the structure and completeness of formal definitions, and a controlled vocabulary of permitted terms for formal definitions.
    - Standard data elements and relationships should be placed into an ACE common data structure.

Since 1991, STC has been developing recommendations for data administration in ACE. The paper is currently a draft technical note, ***Recommendations for ACE Data Administration***, TN-444, Draft Version 1.2 [Ref. STC TN-444 1993]. The report aims to serve as conceptual guidance in the establishment of data administration for ACE and proposes a definition of data administration activities, the methods to be applied, the support facilities required, and an organizational structure and activity plan for starting the establishment of ACE data administration.

Data administration is defined in STC TN-444 as referring to the non-technical activities of planning and implementation for the database environment. These activities include the prescription of policies and standards, planning and coordination, conflict resolution, logical database design, and security control. At present, there is no assigned responsibility for ACE data administration. There are some regional data administration activities, but these activities are not guided by ACE standards. Further, project-related data definition activities are uncoordinated. [STC TN-444 1993]

Work conducted in support of the system design and integration contract (SD&IC) for the ACE ACCIS on data models had the following deficiencies: lack of traceability between sources (messages, directions, etc.) and the data model; lack of integration (the data model is basically message oriented with little cohesion between the "message models"); and lack of completeness (the data model was based on a subset of sources that did not cover all relevant information requirements). The most successful data standardization activities taken so far within ACE and NATO (and among the NATO nations) appear to be in the context of message standards (the work in ATCCIS is an exception to this observation). However, the standards [e.g., ADatP-3, ACE Directive (AD) 80-50, regional supplements to AD 80-50] are inconsistent. [STC TN-444 1993]

6.3.2.6 NATO Publications on Data Management

AAP-6, *NATO Glossary of Terms and Definitions (English and French),* standardizes terminology used throughout NATO, thereby promoting mutual understanding. The criterion for inclusion is that the term be of a general military application. While earlier editions put qualifiers immediately following the term, such qualifiers are now embedded in the definition. In addition, terms and definitions are not to be composed of, nor contain, abbreviations and acronyms. A term and definition are included in the glossary only when they have been agreed upon by all nations in both English and French.

The terms defined in ADatP-2 [Ref. ADatP-2 1985], *Automatic Data Processing (ADP) NATO Glossary, English and French,* are derived from glossaries, dictionaries, and vocabularies from ANSI, American National Directory for Information Processing, ISO, International Business Machines, and ACP 167. The definitions are annotated by source and may include abbreviations, examples, notes, diagrams, accepted synonyms, contrasting terms, related terms, and cross-references for multiple uses. This information is noted when harmonization is being examined for multiple uses.

ADatP-3 (STANAG 5500) [Ref. ADatP-3 1986], *NATO Message Text Formatting System (FORMETS),* provides the rules, constructions, and vocabulary for standardized character-oriented message text formats that can be used in both manual and computer-assisted operational environments.

ACP 167 [Ref. ACP 167 1981], *Glossary of Communications-Electronics Terms,* provides definitions of terms used by communications, electronic warfare, and operational personnel for Allied networks.

6.3.3 Data Management Issues in EDI

The Special Working Group on Electronic Data Interchange (SWG-EDI) of JTC1 has identified a number of data management issues that require coordination within JTC1 (SCs 14, 18, 21, and 24) and with other Technical Committees (TCs) such as TC 46, 68, 154, and 184. The issues include [Ref. SC21 N 3925 1989]:

- Ensuring a complete separation of the semantics and form of data elements, for which the conceptual schema is defined at a level other than the actual applications
- Accommodating different types of data representations, specifically with regard to the data models for different types of data, so as to assure that logical relationships between data of different types can be expressed

- Structuring precisely the dictionaries of data elements and groupings, to include all the attributes of data elements and to permit unambiguous reference to other directories
- Assuring coherence of dictionaries across time (updating and maintenance) and sectors, and also with generic dictionaries.

6.3.4 Data Management for Distributed Applications

The Workshop on Distributed Applications held by JTC1 in March 1990 noted that "very similar data management requirements are being addressed by differing standards applications" and that "potential exists for prevention of a considerable amount of duplication of effort and overlap...by increasing the extent of utilization of common aspects of data management facilities." Coordination was recommended among SC21/WG3 (Database) and WG7 (ODP), SC14, SC18, SC22, SC24, SWG-EDI, TC46, and ITU-TS SGs VII and VIII. Table 8 identifies common requirements for data structures and data models being addressed in ISO. [Ref. SC21 N 4524 1990]

Table 8. Data Management Requirements Identified in ISO Relating to Data Structures and Data Models

• Federated data models
• Mapping to user-oriented data structures/operations
• Ability to support access control to data structures
• Wide range of sizes—large and small volumes of data
• Logging of operations for audit
• Ability to combine separately defined data types (static and dynamic)
• Application-oriented operations (e.g., searching)
• Support for internationalization
• Version control (including data structure modifications)
• Distribution, transparency support, and modelling location
• Handling of uninterpreted data
• Support of different levels of consistency and data integrity
• Ability to relate families of specifications for different levels of abstraction
• Support for recursive and structured definitions
• Persistent storage of results of operations
• Ability to support pointer types
• Ability to support powerful query languages
• Support for Directed Acyclic Graphs (including selection)
• Support for uniqueness requirements
• Independence from programming languages and means of access
• Support of declaration of hotspots and triggers
• Choice of granularity

Source: *Consideration of the Data Management Component of Application Standards*, Workshop on Distributed Applications [SC21 N 4524], April 1990.

A special WG3 ad hoc meeting in May 1992 on the question on distributed database (Q3/007) addressed two future alternatives: (1) that distributed database be considered a very broad topic with required liaison and cooperation with other parts of WG3, especially ODP, or (2) that distributed database be narrowly scoped with possibly a piece in RDA and a piece in SQL. No conclusion was reached and the question will remain open pending further contributions. A further meeting was held in June 1993 in Yokohama, Japan immediately prior to the WG3 meetings. [Ref. SC21 WG3 N 1430 1992]

6.4 Assessment of Coverage by Standards

Data management services include the data dictionary/directory component for accessing and modifying data about data (i.e., metadata), the database management system component for

accessing and modifying structured data, and the distributed data component for accessing and modifying data from a remote database. [Ref. APP 1993]

While the ANSI standard (ANSI X3.138-1988) and FIPS 156 are the same, ISO is working on an Information Resource Dictionary (IRDS) specification (*IRDS Framework*, ISO 10027) that is significantly different in some respects from the ANSI standard. FIPS 156 does not completely specify interface services for a data dictionary/repository—it specifies only the user interface. ANSI X3.185 (ISO 10728), *IRDS Services Interface*, provides an API to IRDS and is appropriate for metadata interchange with a DBMS and between an IRDS and application programs. ANSI X3.195, *IRDS Export-Import File Format*, supports schema and metadata interchange among IRDS-compliant databases, among IRDS and CASE tools with repositories or dictionaries, and between IRDSs and application programs. Additional functionality is needed for IRDS, to include the capability to manage object-oriented data structures and to provide for enhanced communication of information between applications and other data management tools. A major revision of IRDS, sometimes called IRDS2, is underway and is expected to provide such functionality.

A standard relational DBMS interface is provided by *Database Language SQL* (FIPS 127-2 and ISO 9075:1992, sometimes known as SQL2), which incorporates ANSI X3.138:1989 *(SQL)* and ANSI X3.168 *(Embedded SQL)*, together with additional features for schema manipulation, dynamic SQL, exception handling, enhanced integrity constraints, transaction management, and data administration. Not yet addressed are access to remote heterogeneous sites (see below on RDA) and distributed database management. Also needed are tools for the support of object-oriented data management, such as triggers, assertions, user-defined types, domain and table hierarchies, and stored procedures. While the scope of SQL3 (whose standard is expected to be agreed in 1995) is not yet defined, it is expected to support some of these requirements.

Distributed database access is supported by *Remote Data Access*, ISO 9579. RDA is used to establish a remote connection between an RDA client, acting on behalf of an application program, and an RDA server, interfacing to a process that controls data transfers to and from a database. The goal is to promote the interconnection of applications with database systems within heterogeneous environments, with emphasis on an SQL server interface that can provide interoperability between different SQL servers. The client/server approach of RDA is one of several architectures for remote access; others may emerge in data management standards. RDA as yet only specifies the service and protocol between a single client and a single server—it does not currently specify distributed database access, nor does it support stored database procedures.

The US DoD has embarked on an ambitious program to centralize data administration and to define and adopt DoD-wide standard data elements. DoD instructions and procedures have been prepared, but most are as yet only in draft form. A DoD data repository capability has been created, but to date, only a few model-derived prime words and data elements have been approved. Development of data models (e.g., using the DoD-mandated IDEF language) for information systems has only just begun.

(This page intentionally left blank)

7. DATA INTERCHANGE SERVICE STANDARDS

Data interchange services transfer data that represent abstract objects such as military orders, reports, research documents, graphical items (e.g., maps and overlays, symbolic graphical data that might be produced by a simulation), and raw video (e.g., television images). Data interchange services also address product descriptions. An overview of the status of standards for data interchange services is given in Table 9.

7.1 Document Exchange

This section summarizes standards for office document interchange architectures and formats.

7.1.1 Office Document Architecture (ODA) and Interchange Format (ODIF)

Like any object in the object-oriented world, a document contains information relating to its structure and content. A document architecture is a set of rules for defining the structure and representation of a document. It consists of a structural model and a descriptive representation. The structural model describes the structural elements of a document and the relationships among these elements. The descriptive representation describes how the structural elements are represented by attributes.

A content architecture is different from a document architecture. When a document content is thought of as partitioned into content portions, a content architecture defines

Quick Reference

Table 9. Status Overview of Key Data Interchange Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
ODA/ODIF/ODL	●		●	○	○		○
SGML	●		○	●	●		○
SPDL	●		●	●	●		●
EMPM	●	○	●	●	●		○
CGM	●	●	●	●	●	●	●
IGES	●	●		○	●	●	●
STEP			●				
SDTS	○	○	●	●	●	○	●
EDI	●	●	●	●	○	●	○

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key: ● High Evaluation; ○ Average Evaluation; Blank Low Evaluation

Source: [Ref. APP 1993]

rules for positioning content portions within a document. For example, it specifies the nature of the content, the presentation attributes, the coding methods, the control functions that can be applied to the content elements within a content portion, and the content positioning rules. Since a document may contain mixed contents (e.g., text and graphics), different content portions with different content architectures can coexist within a document. So far, three different content architectures have been defined by the Office Document Architecture (ODA) standard. They are:

- Character Content Architecture—supports the character repertoire defined in ISO 6937 (*Coded Character Sets for Text Communication*) and other character sets as long as they are defined according to the rules of ISO 2022 (*ISO 7-bit and 8-bit Coded Character Sets - Code Extension Techniques*).
- Raster Graphics Content Architecture—supports raster graphics, which represent images as pixels or, in ODA terms, pels (picture elements).
- Geometric Graphics Content Architecture—supports a content type consisting of a series of geometric constructs such as point, lines, arcs, polygons, etc. The geometric graphics in ODA are based on ISO 8632 (*Computer Graphics Metafile for the Storage and Transfer of Picture Description Information*).

Future versions of ODA standard may include content architectures for sound, speech, and three-dimensional images. [Ref. Tang 1992]

ODA (ISO 8613) was originally designed for the interchange of office documents between different word processors. The equivalent ITU-TS Recommendations are the T.410 series (see end of Appendix E). ODA describes a document in terms of its logical structure or its layout structure or both together. The ODA standard is divided into several parts:

- ISO 8613-1 (Part 1), *Part 1: Introduction and General Principles*
  - AM 1, *Document Application Profile Proforma Notation*
  - AM 2, *Conformance Testing Methodology*
- ISO 8613-2 (Part 2), *Document Structures*
  - PDAD 1, *Formal Specification of ODA Document Structures*
- DIS 8613-3 (Part 3), *Abstract Interface for Manipulation of ODA Documents*, April 1993
- ISO 8613-4 (Part 4), *Document Profile*
- ISO 8613-5 (Part 5),*Office Document Interchange Format (ODIF)*
- ISO 8613-6 (Part 6), *Character Content Architectures*
- ISO 8613-7 (Part 7), *Raster Graphics Content Architectures*
- ISO 8613-8 (Part 8), *Geometric Graphics Content Architectures*
  - DAD1, *Tiled Raster Graphics*
  - DAM 2.2, *Color*
  - DAD 3, *Alternative Representation*
  - DAD 4, *Security*
  - DAM 5.2, *Streams*
  - DAD 6, *Styles*
  - PDAM 10, *ODA External References and Document Fragments*
- CD 8613-9 (Part 9), *Audio Content Architectures*
- ISO/IEC 8613-10 (Part 10), *Formal Specifications*
  - AM 1, *Formal Specification of the Document Profile*
  - AM 2, *Formal Specification of the Raster Graphics Content Architectures*
  - AM 3, *Formal Specification of ODA Character Content Architectures*, 1992

- AM 4, *Formal Specification of ODA Geometric Graphics Content Architectures*, 1992
- AM 5, *Formal Specification of the Defaulting Mechanism for Defaultable Attributes*, 1993.

- CD 8613-11 (Part 11), *ODA Spreadsheet*, April 1993
- DIS 8613-12 (Part 12), *ODA Identification of Document Fragments*, April 1993.

Part 5 of ODA specifies a second method of representation and interchange, using the Office Document Language (ODL) and the Standard Generalized Markup Language (SGML) Document Interchange Format (SDIF). ODL is an application of SGML, and may be used to represent a document structure in accordance with ODA in SGML. (SGML is discussed in Section 7.1.2 below.)

In 1993, ISO adopted TR 10183-1, *Text and Office Systems - ODA and Interchange Format - Technical Report on ISO 8613 Implementation Testing.*

ISO 8613 is being adopted as an American National Standard as well. ANSI X3V1, Text: Office and Publishing Systems, plans to produce multiple part addenda that will provide extensions to an ANSI standard that will remain consistent with the ISO 8613 standard. [Ref. X3 1991] The following describes this new work [Ref. OSN 1991k]:

- Revision accountancy consists of a collection of several revisions of a document, possible including some additional information as to the status and rational for a revision and its author.
- Annotations may or may not form a permanent part of a document, but they may use any content type.
- Automatic content generation refers to generated listings including table of contents, tables of figures, and illustrations; indexes and glossaries; cross references; and copying of body material into executive summaries and outlines.
- ODA business charting includes the ability to derive a business graphic from tabular, spreadsheet or other data in the document or referenced by the document; derive part of a document from an external business graphic; and include a business graphic in a document in such a way that the business graphic specific processing can be performed by the recipient.
- Hypermedia structures allow an originator to be able to pass to a recipient the intention that the recipient can follow one or more routes through the logical structure with associated control of the presentation of an ODA document.
- The ODA audio content architecture (Part 9) will define a content architecture for voice and other audio information. It will use pre-existing or developing coding standards for audio. Audio content, which may be used for annotation or other purposes within a document, has a close relationship with time synchronization and annotation extensions for the ODA document processing work.

The Profile Alignment Group for ODA (PAGODA) has been formed from the three special interest groups (SIGs) and expert groups (EGs) from the three regional OSI workshops (see also Section 16.1.1): Asia/Oceania Workshop (AOW) ODA SIG, EWOS ODA EG, and the NIST ODA SIG. PAGODA is developing ODA profiles based on ISO 8613, *Office Document Architecture (ODA) and Interchange Format (ODIF).* The Office Document Format (FOD) provides for two types of structure in its proposed taxonomy [Ref. SGFS 1989]:

- Hierarchically related based on increasing complexity and functionality (simple, enhanced, and extended document structures). The simple document structure is intended to address the general requirements of current word processing applications.

The enhanced document structure is intended to address the general requirements of emerging word processing applications that have been enhanced over current applications. The extended document structure would address the general requirements of emerging personal publishing and document processing applications.

- Content architectures for various combinations of character, raster graphics, and geometric graphics content architectures.

Profiles that have achieved International Standardization Profile (ISP) status (see Section 16.1.2.4) include the following [Ref. OSN 1991c]:

- FOD11 (ISP 10610-1), *Office Document Format Profile for the Interchange of Basic Functional Character Content Documents in Processable and Formatted Forms* - Part 1: *Document Application Profile (DAP)*, April 1992
- FOD112 (pDISP 12064-1), *Open Document Format: Image Applications - Simple Document Structure - Raster Graphics Content Architecture,* Part 1: *FOD 112, Document Applications Profile,* August 1993 (balloting ended December 1993)
- FOD26 (ISP 11181-1), *Office Document Format Profile for the Interchange of Enhanced Function Mixed Content Documents in Processable and Formatted Forms* - Part 1: *Document Application Profile (DAP)*, April 1992
- FOD36 (ISP 11182-1), *Office Document Format Profile for the Interchange of Extended Function Mixed Content Documents in Processable and Formatted Forms* - Part 1: *Document Application Profile (DAP),* April 1992.

Although there is no strong user demand for ODA products, predictions are that over the next 5 years ODA has the potential to satisfy growing demand for standards-based document management, particularly interchange. Three types of ODA products are available:

- ODA toolkits—intended to enable ODA conversion facilities to be built into products and systems with minimum effort
- Converters—extensions to existing products to allow them to take part in ODA document interchange
- Native products—applications that implement document processing functions that conform to ODA standards.

Six major international computer companies formed the Open Document Architecture Consortium (ODAC) to develop a toolkit of software that conforms to the ISO ODA standard. The companies are Digital, ICL, Siemens Nixdorf Information Systems, Group Bull, IBM, and Unisys. The toolkit was expected to be available in 1993 [Ref. OSN 1991b]. In addition, Apple Europe has made available an ODA toolkit called WOPODA.

Bull, Siemens-Nixdorf, and Xerox offer ODA converters as part of their more comprehensive office systems products. Beta test versions of word processor converters and native ODA editors are in use on personal computers and the Apple Macintosh.

ODA has been the subject of visible interworking demonstrations both in Japan and Europe. Cooperative activity in Europe has included the PODA (piloting ODA) project that, in 1990, demonstrated the interchange of integrated text and graphics documents between participants systems using X.400 electronic messaging. Moreover, IBM recently announced that it will adopt the ODA standard instead of the revised form of its own Mixed Object Document Content Architecture (MO:DCA). Microsoft has also declared its intention to support ODA and has an ODA Manager based around its Microsoft Word product. [Ref. OSN 1991d]

7.1.2 Standard Generalized Markup Language (SGML)

SGML formalizes document markup, making the document system and processing independent. It is an architecture-free and application-free language for managing structures and is designed for full multimedia database publishing. SGML is a meta-language, providing the rules for designing and applying a system of markup tags rather than the specific set of tags. As noted above, ODL is a set of rules in ODA for using SGML to represent documents. The SGML standards are:

- ISO 8879, *Standard Generalized Markup Language (SGML)* (FIPS 152)
- TR 9573, *SGML Support Facilities—Techniques for Using SGML*, which is under revision to include the following parts, all of which are in WD status except Parts 11 and 12, which have reached TR status:
  - Part 1: *SGML Tutorial*
  - Part 2: *Basic Technique*
  - Part 3: *Advanced Techniques - Using LINK and CONCUR*
  - Part 4: *Advanced Techniques - Using SHORTREF to Indicate Markup*
  - Part 5: *Using Non-Latin Alphabets*
  - Part 6: *Referencing and Synchronization*
  - Part 7: *Mathematics and Chemistry*
  - Part 8: *Tables*
  - Part 9: *Using SGML for Computer to Computer Interchange*
  - Part 10: *Designing Applications for Database Interfacing*
  - Part 11: *Application at ISO Central Secretariat for International Standards and Technical Reports: 1991*
  - Part 12: *Public Entity Sets for General and Publishing Symbols: 1991*
  - Part 13: *Public Entity Sets for Mathematics and Sciences*
  - Part 14: *Public Entity Sets for Latin Based Alphabets*
  - Part 15: *Public Entity Sets for Non-Latin Based Alphabets*
  - Part 16: *Public Entity Sets for Ideograms*
- ISO 9069, *SGML Support Facilities—SGML Document Interchange Format*
- ISO 9070, *SGML Support Facilities—Registration Procedures for Public Text Owner Identifiers*
- TR 10037, *SGML and Text-Entry Systems—Guidelines for SGML Syntax-Directed Editing Systems.*

X3.190-1992, *Conformance Testing for SGML*, addresses the construction and use of test suites for verifying conformance of SGML systems (see also Section 12.2). Its provisions assist those who build test suites, those who build SGML systems to be evaluated by such suites, and those who examine an SGML system's performance on a test suite as part of the process of selecting an SGML tool. [Ref. X3 1991a]

Three standards related to SGML are:

- ISO 10179, *Document Style Segmentation and Specification Language (DSSSL)*, June 1991
- DIS 10180, *Standard Page Description Language (SPDL)*, March 1991 (a FIPS is planned by NIST)
- MIL-M-28001B, *Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text*, June 1993.

Some people believe that these standards, when used with SGML and viewed as a group, will comprise a much more comprehensive information management architecture than that envisioned by ODA. [Ref. Terrell 1990]

HyTime. SGML is also being extended to deal with hypermedia/time-based document interchange. The HyTime standard, *Hypermedia/Time-based Structuring Language (HyTime)*, was developed by ANSI X3V1.8M (Project 749-D) and ISO (ISO 10744). It is a notation to describe hypermedia. HyTime is a collection of abstract semantic constructs associated with syntactic conventions. It allows hyperdocument interoperability (1) without standardizing multimedia objects, their notations, their modifiers, the effects of those modifiers on them, and the semantics of link types; and (2) without requiring existing documents to be recast in order to make their contents linkable to HyTime documents. HyTime-compliant documents can allow HyTime-cognizant software to browse, render, format, and query them even if that software is not able to understand or render its multimedia objects. If the notation of an object is uninterpretable because no interpreting system is locally available for it, the render can still incorporate some form of blankness, e.g., darkness, silence, or an appropriate error message, so that the space and time relationships of the rendered and unrenderable objects are preserved. [Ref. Newcomb c1991]

HyTime is gaining worldwide acceptance. The US DoD has plans to use HyTime as the basis for its Interactive Electronic Technical Manuals. The European Community has approved HyTime for official projects and has just let a contract to encode their central database for official travel in HyTime. [Ref. CGA 1992]

EMPM. Object-oriented methods are at the heart of another similar standards effort, led by the Multimedia and Hypermedia Information Coding Experts Group (MHEG). [Ref. Fox 1991] The Electronic Manuscript Preparation and Markup (EMPM) specification, ANSI/NISO Z39.59-1988, is an architecture encoded in SGML suitable for the interchange of the logical structure of books, articles, and serials. Developed by the Association of American Publishers (AAP), it provides a high level language for describing these logical structures but offers little assistance with layout and presentation style issues. [Ref. APP 1992].

CALS. SGML has been chosen by the US DoD as the documentation standard for its Continuous Acquisition and Life Cycle Support (formerly Computer Acquisitions and Logistics Support) (CALS) strategy. This strategy is designed to take defense information from its current paper form to a totally electronic mode over the next decade. MIL-M-28001B establishes the requirements for the digital data form of technical publications. Data prepared in conformance to these requirements will facilitate the automated preparation, storage, retrieval, exchange, and processing of technical documents from heterogeneous data sources. The requirements set forth by this specification include:

- Procedures and symbology for markup of unformatted text in accordance with this specific application of SGML
- SGML-compatible codes that will conform a technical publication to specific format requirements
- Output control codes that will conform automated document processing functions to a uniform structure.

MIL-M-28001B establishes the requirements for the digital forms of all US DoD technical publications using SGML. Data files satisfying the requirements of this specification will be one of two types: Type I - MIL-M-38784B conforming technical manuals and Type II - technical manuals conforming to other military specifications. Documents prepared in accordance with MIL-

M-38784B and MIL-M-28001B must conform to the document type definition (DTD) defined in Appendix A and the output specification in Appendix C of MIL-M-28001B. The DTD and output specification for a MIL-M-38784B conforming manual do not have to be delivered with the tagged text. Technical manuals conforming to other military specifications may develop their own DTD but must use only those tags in the baseline tag set defined in Appendix B of MIL-M-28001B. In this case, the DTD must be delivered with the publication along with a compatible output specification.

MIL-M-28001B addresses the five steps in the publication preparation process:

(1) Creating a DTD for publication control

(2) Authoring the publication and inserting SGML markup tags

(3) Verifying the syntax according to the rules of SGML

(4) Using the output specification to compose the document so that produced copy corresponds to the proper formal and style

(5) Generating a text presentation metafile in SPDL to drive the display device.

The heart of MIL-M-28001B is found in its appendixes. Appendix A specifies the role played by the DTD in an SGML implementation; a general description of DTD structure and content; the specific DTDs available for use in authoring, validating, and verifying an SGML-tagged technical document; and procedures for DTD development. The appendix introduction provides an overview of the concepts behind the SGML standard, a brief tutorial on reading an SGML DTD, guidelines for using SGML tags, and DoD's SGML declaration. Two DTDs are also presented in Appendix A. This first DTD is for use when preparing a document that conforms with MIL-M-38784B. The second uses the same elements as the first DTD with the addition of more subordinate paragraphs and steps. This DTD may be used for MIL-M-38784B non-conforming documents or as a model for the development of a more appropriate DTD. Both DTDs allow for four types of non-SGML data: IGES data, CGM data, ITU-TS Group 4 data, and system-generated data.

Appendix B of MIL-M-28001B contains an alphabetical listing of all elements contained in the DTDs presented in Appendix A. Appendix C is a stand-alone document. It includes a document output specification (format and style guide) to be used for all applications of this specification. Although the format default values are set according to MIL-M-38784B, the values may be tailored to satisfy other format requirements. The appendix also provides an example of an SGML-coded source file and the composed sample document produced from the marked up file.

The US DoD CALS Digital Standards Office recently established the CALS SGML Library (CSL) which will be the DoD holding place for all registered and approved SGML tags used in DTDs for functional specifications and other DoD CALS documentation using SGML applications. The CSL will also contain the official DTDs for military specifications as well as other related SGML data not yet defined. Therefore, there is no longer a need to have the MIL-M-38784B DTD and all the subset DTDs from Appendix D, the library entities from Appendix C, or the Baseline Tag Set Table residing in MIL-M-28001. This will considerably streamline MIL-M-28001. [Ref. Barlow Report n.d.]

CALS, since it is an application-specific architecture oriented to technical weapons systems support documentation, may not be applicable to all of the other types of information that a generic information system comprises.

Relation of SGML to ODA. There is an incorrect perception that ODA and SGML are competing standards. In fact, ODA is a generic interchange architecture that uses SGML as one of its interchange formats. The other interchange format, ODIF, is specifically of use in an OSI environment because it uses ASN.1. However, both standards exist in the application layer of the OSI. Although CALS has selected SGML, it has left the door open to ODIF as well. The NIST assessment is that both ODA/ODIF and SGML enjoy an average level of consensus, and neither has much product availability or de facto usage. However, it evaluates ODA/ODIF as being more complete than SGML, but rates SGML as being significantly more stable and mature than ODA/ODIF. [Ref. APP 1991, p. 35]

However, SGML and ODA are incompatible in the sense that most documents encoded using SGML cannot be used directly in an ODA-based system, and vice versa. Translations programs are therefore necessary if both standards are to be used. [Ref. Nicholas 1992]

7.1.3 Distributed Office Applications Model (DOAM)

The *Distributed Office Application Model* (DOAM, ISO 10031) was established to provide a set of common principles to which all Distributed Office Application (DOA) standards must adhere. The two parts of this standard, *General Model* and *Referenced Data Transfer* (see Section 7.1.7) do not contain any implementable protocols; they are limited to the description of models and tools to be used by DOA standards developers.

An important feature of the DOAM is the client-server model, which allows one part of an application to be implemented in a "client" machine and another part to be implemented in a "server" machine. This possibility of splitting an application allows certain central resources, such as a large database or an expensive laser printer to be shared among a number of users from their workstations.

DOA consists of the DOA model (DOAM) and two specific DOAs: *Document Filing and Retrieval* (DFR, ISO 10166; see Section 7.1.6) and *Document Printing Application* (DPA, DIS 10175). The DOAM (ISO 10031) addresses the general model, design guidelines for the peer-to-peer (Application Layer) protocol, and Referenced Data Transfer (*RDT*). Use of ROSE is mandatory in DOAM. The DOAM guidelines are used to define DOA objects (e.g., documents), together with object attributes and criteria for filtering those objects. The DOAM guidelines identify a set of abstract operations such as List, Read, Write, Modify, Copy, Move, Search, Create, Delete, Reserve, Unreserve, Notify, and Abandon. RDT is the mechanism used to perform transfer of objects. RDT was developed to permit "small" systems (e.g., workstations) to handle "large" objects, such as moving an object from a document store to a print service. DFR defines the structure of a document store and an associated access protocol. DPA defines an access protocol for print services. DOA is being developed by SC18/WG1 [Ref. SC21 N 3930 1989]. SC18 merged the DOA and messaging work into one working group (WG4) to produce better cooperation between the two areas. [Ref. OSN 1991k]

A new work item for SC18/WG4 (Special Working Group on DOA) is *Engagement Scheduling and Recording Application (ESRA) with the DOAM,* August 1993 [SC21 N 8255]. It will provide a specification of a service and protocol that supports scheduling and recording of engagement entries on multiple calendars. Part 1, *Abstract Service Definition and Procedures,* was expected to have CD status in 1993, DIS status June 1994, and IS status December 1995.

7.1.4 Electronic Data Interchange (EDI)

EDI[32] provides for a standardized exchange of data between systems by a wide range of means, including exchange of magnetic tapes and the transmission of data by Telex. EDI is intended to enable data to be interchanged without networking and is used mainly for interorganization communication where internetworking may be undesirable (internetworking is a primary feature of OSI).

It is important to note that although the standard focuses on the structure of an EDI document, it leaves the communication community to develop a solution for the transfer of the document, using, for example, the OSI international communication standards (see Chapter 9), to support the exchange of an international interchange format. The benefits of applying OSI to EDI include reduced clerical overhead and faster transmission, which imply lower cost and better service to the customers. [Ref. Tang 1992].

EDI Standards. Prior to 1985, there were two world-wide EDI standards, UN-TDI/GTDI in Europe and ANSI X12 (*An Introduction to EDI*, July 1987) in North America. In 1988, the United Nations Economic Commission of Europe (UN ECE) published the standard *EDI for Administration, Commerce, and Transport (EDIFACT)*, designed to be a single standard for both communities. TC 154 of ISO, which deals with trade and commerce, ratified the EDIFACT syntax and trade dictionary, and produced two ISO documents: ISO 9735 and ISO 7372. Since then, EDIFACT has been widely accepted as a worldwide de facto standard. EDIFACT is based on ISO 646 encoding [7 bits per character—ASN.1 Basic Encoding Rules (see Section 9.10.2) use the full range of 8 bits in each octet]. A large number of standard messages have been developed based on EDIFACT, and the EDIFACT has been endorsed by many standards bodies and user groups.

Another standard, TRADACOMS, has been developed for use in the United Kingdom, based on the UN-GTDI syntax. TRADACOMS is now in wide use in the United Kingdom and currently enjoys the status of de facto UK standard. However, a recent notice [Ref. CCTA 1991a] issued by the CCTA in the United Kingdom states that "departments should refrain from its (TRADACOMS') use" and invites departments and agencies to adopt EDIFACT as the EDI standard. CCTA's UK GOSIP Version 4 provides up-to-date guidance on the use of EDIFACT.

EDIFACT provides data structure and content standards for developing messages for use by importers, exporters, transportation firms, financial institutions, ports, customs, and other business and administrative activities (e.g., insurance, tourism, construction). EDIFACT was developed by the UN working party on Facilitation of International Trade Procedures to ensure there is only one worldwide standard for EDI. EDIFACT is ISO 9735 and uses the international standard Trade Data Element Directory (ISO 7372) [Ref. SC21 N 3885 1989]. ANSI X12 guides, stimulates, and promotes the development and use of the EDIFACT standards in the United States and Canada, but EDIFACT is still not aligned with ANSI X12. The ANSI X12 Secretariat has noted that differences in syntax control segments, data segments, and data elements continue to exist between EDIFACT and the X12 standard for EDI [Ref. DISA 1990]. X12 plans to align with EDIFACT in 1997, after publication of Version 4 of the X12 standards in 1994. [Ref. Kornfeld 1990] FIPS 161 (EDI) was published 29 March 1991.

32 The abbreviation EDI is frequently written in all-lower-case letters: edi.

Use of EDI in MHS and FTAM. Either the Message Handling System (MHS) standard (ITU-TS X.400) or the File Transfer, Access, and Manipulation (FTAM) standard (ISO 8571) can be used to transfer an EDI document. In particular, the security features of the 1988 version of the MHS standard are of great importance to the business world. Therefore in 1990, CCITT brought together MHS and EDI, and produced two CCITT Recommendations, namely, F.435 and X.435. F.435 describes the MHS-EDI messaging service, while X.435 describes the MHS-EDI Messaging System in more depth. The framework of the 435 documents is general in the sense that it uses MHS to carry not only EDIs conforming to EDIFACT, but also EDIs conforming to TDCC, ANSI X12, and others. It is robust because it can be used to carry EDI documents of different formats in the future.

In 1991, ITU-TS published X.435, *Message Handling Systems: Electronic Data Interchange Messaging System*. X.435 uses a new User Agent protocol called PEDI that includes security services necessary to support nonrepudiation. The ITU-TS EDI user agent allows CALS formats (e.g., US MIL-STD-1840B, *CALS Originator File Sets and Transfer*) to be supported as body parts.[33]

In May 1991, SC21/WG5 proposed an EDIFACT/FTAM Document Type (see also Section 9.11.6) in an attempt to merge existing FTAM implementations with existing EDI systems with a minimum of change. [Ref. SC21 N 6224 1991]

Use of EDI in CALS. The CALS initiative is the largest and best known of the EDI proponents. CALS required full compliance to EDI standards for digital delivery of technical information and interoperability among DoD systems beginning in January 1990. Major applications areas are automation of technical manuals, computer-assisted design, and spares acquisition. CALS standards include EDI for data interchange file management, IGES for engineering drawings, Standard Generalized Markup Language (SGML) for automated publishing, and CGM for technical manual illustrations. The standard currently being used for raster graphics representation is US DoD-unique (MIL-R-28002B dated 14 December 1992).

MIL-HDBK-59B, *Department of Defense Computer-aided Acquisition and Logistic Support (CALS) Program Implementation Guide* (dated 12 June 1993) assists weapon system acquisition managers to understand when, where, and how to apply CALS capabilities efficiently to support their information interchange and access requirements, and how to define their functional requirements for integration of the contractor processes (such as reliability and maintainability analysis) that create and use the information.

MIL-STD-974, *Contractor Integrated Technical Information Service (CITIS), Functional Requirements* (Fall 1993) implements the DoD's new CALS acquisition policy, which gives preference to contractor information services and on-line access instead of data deliverables. While the other CALS standards address the transition from paper data deliverable to digital data deliverables, MIL-STD-974, addresses how DoD will buy information services. It defines things a contractor must do, such as planning, analysis, and submitting proposals, and things the service must do, such as managing data, and providing access to the data tailored to meet a government Concept of Operations.

---

33 The *Report on ITU-TS Study Group 7 Program of Work and Collaboration with SC 21*, SC21 N 7887, June 1993 lists X.435 as an "Independent" project and does not indicate that ISO intends to adopt this standard. Likewise, *SD-10: SC21/ITU-TS Collaborative Projects*, SC21 N 8083, September 1993 does not list it.

MIL-ACQ-GUIDEA, *Acquisition Guide for Implementation of Computer-aided Acquisition and Logistic Support (CALS)*, provides information to personnel responsible for the acquisition and use of weapon system technical data. Its purpose is to assist acquisition managers in making the transition from paper-intensive processes to digital data delivery and access. It also supports the structuring of contract requirements to achieve integration of various contractor automated capabilities for design, manufacturing, and logistic support. [Ref. CALS/CE 1992a]

A Tri-Service Working Group produced three military specifications on Interactive Electronic Technical Manuals (IETMs), one of the fastest growing areas in CALS to be tested and implemented. They are [Ref. CALS 1993]:

- MIL-M-87268, *IETMs: General Content, Style and Format*
- MIL-D-87269, *Interchange Formats for IETM Databases*
- MIL-Q-87270, *Requirements for Quality Assurance Programs for IETMs.*

Open-EDI. The ISO/IEC JTC1 special working group (SWG) on EDI published a report on the Open-EDI [JTC1 N 1384 May 1991] conceptual model for furthering global interoperability of electronic data interchange. The "open-EDI" model (1) describes "business" relationships among participants in EDI in a formal way and (2) facilitates development of standards and tools supporting this description. The report recommended seven new work item proposals:

- Open-EDI Reference Model
- Business Agreement Services
- EDI Support Services
- Requirements for Amendment and/or Addition of Non-EDI-Specific Standards
- Usage Specifications for Non-EDI-Specific Standards
- Requirements for Amendment and/or Addition of EDI-Related Standards
- Usage Specifications for EDI-Related Standards.

Moreover, the report recommended that this work be conducted under responsibility of a single body. Since no single existing subcommittee had a scope which covers all aspects concerned, the JTC1/SWG-EDI recommended that a new subcommittee called Open-EDI be formed to take responsibility for development of a conceptual model for EDI and of associated standards, and for furthering global interoperability of EDI. JTC1 disbanded the SWG-EDI and resolved to establish a Working Group to work on open-EDI with the title, scope, and program of work recommended by the SWG-EDI. [Ref. SC21 N 6530 1991]

Consequently, the Inter-Agency edi Working Group (IAeG) was formed, bringing together representatives from the UN, ITU-TS, and JTC1. The October 1992 meeting produced a temporary document (IAeG N 32 R2) which includes proposals for discussion. It also suggests a matrix of technical areas subject to standardization linked to the organizations who produce standards today, and proposes a new distribution of work in these areas. [Ref. SC21 N 7487 1992]

At the request of the JTC1 WG3 open-EDI group, the Special Working Group on Modeling Facilities (SWG-MF) (see Section 6.2.5.3) issued tentative working definitions and distinctions between the meanings of the terms conceptual schema modelling facility (CSMF) and data modelling facility (DMF), as well as interim guidelines for using conceptual modelling facilities, and for specifying standards. These definitions are contained in [Ref. SC21 N 7542 1993] and provided in Section 6.2.5.3.

In July 1993, the British Standards Institute highlighted [Ref. DISC 1993a] the confusion created by multiple standards-making bodies for EDI. These include, as noted, the United Nations and its Economic Commission for Europe, the Simplified Trade Procedures (SITPRO) organization under the UK DTI, the technical committees of ISO that develop bar coding and other standards, and the ISO/IEC JTC1 that develops the underlying information technology standards. In addition, there is the Western European EDIFACT Board, which operates on behalf of the United Nations, a CEN ad hoc working group on EDI, and a CEN working group on CALS. Since that report, EWOS has created an expert group focusing on EDI.

A comprehensive analysis of EDI user requirements and survey of current activities are provided in the *EWOS Technical Guide on EDI* [Ref. ETG 30 1993]. Current concerns regarding EDI are the data transfer aspects, in particular the interface between EDI applications and communications protocols in an open systems environment (OSE). The EWOS Expert Group (EG) on EDI, initiated in September 1993, is responsible for the technical work of EWOS in the area of EDI, including communications support. [Ref. EWOS/TA/93/331 1993] One new work item proposal for the EG-EDI is, *Interactive EDI and TP*, developing TP OSE profiles for use by EDI applications (target date is September 1994). Of specific concern by users is multiparty operation, such as in passenger airline reservations and cargo reservation systems. A parallel new work item proposal is on *Profiling Methodologies for Composite EDI Message Structures*, in which there may be data encoded in a variety of standards or de facto specifications that need to be embedded in an EDI message target date is May 1995). These may include graphic designs and image-plus-character-based information. A future requirement may be full-motion, full-picture video.

7.1.5 Document Transfer and Manipulation (DTAM)

DTAM is being developed by ITU-TS SG8. The DTAM protocols are designed to support interactive as well as store-to-store real-time end-to-end communications. They are also suitable for multimedia applications. Telematic applications are currently defined within the integrated, modular approach based on ODA (see Section 7.1.1), DTAM, and Document Architecture Operations (DAO, ITU-TS SG VIII). The telematic applications are Group 4 Facsimile, mixed mode, processable mode, and videotext internetworking. Each telematic application consists of equipment characteristics, document characteristics (selected from ODA), operational characteristics (optional, selected from DAO), and communications characteristics (selected from DTAM).

DTAM differs from FTAM in that the standards address different environments. FTAM satisfies requirements for the transfer of files between different file systems, including retention of generic filing information. DTAM, on the other hand, provides facilities for the storage, management, and retrieval of documents in an integrated office application environment.

Two types of telematic and office environment applications for DTAM are being developed by ITU-TS SG8 and ISO JTC1 SC18: conference type and remote document handling. A service called Remote Open Document Editing (RODE) is being proposed for the telematic environment to provide real-time remote editing for content manipulation through use of ODA/DTAM. RODE is expected to fulfill such user requirements as observing changing documents; maintaining identical documents between partners, even when partners have different presentations; providing speedy manipulations; and potentially supporting participation of more than three partners. Services are

being defined to enable RODE to support a desk top conference application using DFR as well as RODE. [Ref. SC21 N 4342 1990]

7.1.6 Document File and Retrieval (DFR)

DFR (ISO 10166) is the responsibility of ISO/IEC JTC1 SC18/WG4. DFR is one of the office application standards defined by the DOAM (see Section 7.1.1) and shares common mechanisms with Directory services and MOTIS. These mechanisms include attribute definition and filtering facilities, and they use the Remote Operations Service Element (ROSE) and the Reliable Transfer Service Element (RTSE).

DFR also supports a "version management" mechanism. This mechanism allows a document to be declared as a new version of an existing document. When this is done, a "previous-version" attribute points to the previous version of the document, and the previous version correspondingly receives a "next-version" attribute, thus retaining the complete evolution of a given document. All versions of a document contain a "version-root" attribute indicating the first version of the document.

ISO 10166, *Document File and Retrieval*, has the following two parts:

- ISO 10166-1 (Part 1): *Abstract Service Definition and Procedures*, 1989
- ISO 10166-2 (Part 2): *Protocol Specification*, 1989.

DFR and DTAM both handle primarily ODA documents. They differ in that DFR is not concerned with the inner content of a document, whereas DTAM is concerned with both the whole document and the inner content of the document. Further, DFR provides for filing and retrieval of (whole) documents, whereas this capability is not supported by DTAM.

DFR differs from FTAM in that filing and retrieval of documents is DFR's single specific office application. An important difference between these two standards is the manner in which a document or file is identified. DFR uses a "Unique Permanent Identifier" that remains with the object for its lifetime. FTAM uniquely identifies its objects by its pathname from the root through the directories leading to it. In FTAM, if the contents of a file are moved to another directory, the pathname will change. Also, there is no analogy in FTAM of DFR's version control mechanism.

A joint meeting between SC21/WG5 (FTAM) and SC18/WG4 (DFR) in Stockholm in May 1989 concluded that, due to the different user requirements being met by the two standards, a general-store model could not be progressed. [Ref. OSN 1989a]

7.1.7 Referenced Data Transfer (RDT)

RDT standards have been developed by ECMA TC32-TG5 and ISO/IEC JTC1 SC18/WG4. The RDT protocol duplicates functionality provided by FTAM, specifically the simple, efficient transfer of unstructured data (this is provided by FTAM-3 and the FTAM Transfer Service Class). However, a minimal implementation of FTAM would not provide all the apparent RDT requirements, such as security, single/multiple use of reference, finite life of reference, and use over a single association along with the RTSE. ISO 10740, *Information Technology - Text and Office Systems - Referenced Data Transfer*, which was approved in 1993, has the following parts:

- ISO 10740-1 (Part 1): *Abstract Service Definition*
- ISO 10740-2 (Part 2): *Protocol Specification*.

7.1.8 DoD Document Exchange Standards

The US DoD has developed the following standards for document format and exchange:

- DoD-STD-7935, *Automated Data Systems (ADS) Documentation*, February 1983
- MIL-M-38784B, *Manuals, Technical: General Style and Format Requirements*, February 1991
- MIL-STD-1840B, *Automated Interchange of Technical Information*, November 1992
- DoD-STD-2167A, *Defense System Software Development*, February 1988.

DoD-STD-7935 provides guidelines for the development and revision of the documentation for Automated Data Systems (ADS) of applications computer programs, and it prescribes the standards and descriptions for each of the technical documents to be produced during the life cycle of an ADS. ADS is defined as "an assembly of procedures, processes, methods, routines, or techniques (including, but not limited to, computer programs) united by some form of regulated interaction to form an organized whole, specifically designed to make use of automatic data processing equipment." The objective of the standard is to provide managers of ADS projects with documentation of uniform format and content for review to assure the meeting of significant development milestones. It also provides ADS technicians with a standard record of technical information as a basis for coordination of later ADS development or use modification. There are 11 technical documents described in the standard: Functional Description, System/Subsystem Specification, Data Base Specification, Computer Operational Manual, Test Plan, Implementation Procedures, Data Requirements Document, Program Specification, Users Manual, Program Maintenance Manual, and Test Analysis Report. A proposed outline and text format for each document type is provided in Section 3.0 of the standard.

MIL-M-38784B is a military specification approved by the DoD for use in developing technical manuals. Technical manuals are publications that contain instructions for the installation, operation, maintenance, training, and support of weapon systems, weapon system components, and support equipment. Manuals prepared in accordance with this specification are intended for use in the operation and maintenance of equipment or for accomplishment of assigned missions. It covers the general style and format requirements for the preparation of manuscripts and reproducible copy for standard technical manuals and changes to those manuals. The only decision left to the author of a technical manual is the actual technical content of the manual; even the style of writing is specified (US Government Printing Office Style Manual).

The major section of MIL-M-38784B, Section 3.2, is dedicated to format issues. The specification covers everything from the size of the paper to capitalization to suggested type styles and sizes. The specification identifies the structure of a technical manual. It specifies what will be included in the manual outline and publication divisions (volumes, parts, chapters, sections, and paragraphs). Paragraphs are divided into primary and subordinate paragraphs. The last sections of the specification discuss how to make changes to a technical manual, quality assurance provisions (e.g., readability), and preparation for delivery (packaging).

The purpose of MIL-STD-1840B is to standardize the digital interface between organizations or systems exchanging digital forms of technical information necessary for the logistic support of weapon systems throughout their life cycle. This standard addresses technical information and product definition data. It standardizes the format and information structures of digital data files used for the transfer and archival storage of digital technical information. The format, information structures, and transfer procedures are applicable in all cases where the

information can be prepared and received in the form of American Standard Code for Information Exchange (ASCII) text files, product definition data files, raster image files, or graphics files.

Technical publications addressed by MIL-STD-1840B consist of text and associated illustrations. The files of a technical publication consist of a declaration file, text files (in ASCII) tagged to the contract (may use MIL-M-28001B), illustration files (in Initial Graphics Exchange Specification (IGES), Computer Graphics Metafile (CGM), or raster format), files in Page Description Language (PDL) form, and other files (output specification file, special word file, etc.). The standard dictates very detailed requirements for the structure, content, and order of information. For example, the declaration file must precede the data files and provide information about the identifications, source, destination, and classification of the document. The standard also specifies the file header records for textual data, CGM data, document type definition, program descriptive language (PDL) data, IGES data, gray scale, raster data, special word, and output specification data.

DoD-STD-2167A provides the means for establishing, evaluating, and maintaining quality in software developed for weapon systems and its associated documentation. The contract agency is responsible for tailoring the software management process to meet the needs of a particular project. The data item descriptors (DIDs) associated with this standard describe a set of documents for recording information required by the management process. The standard encourages the production of deliverable data using automated techniques.

7.1.9 Data Descriptive File[34]

ISO 8211, *Specification for a Data Descriptive File for Information Interchange*, December 1985, has potential value for data interchange as a medium-independent and system-independent file and record format. It could be used, for example, for interchange of graphical data structures and files between computer systems. It could also be used for exchange of geographical data. There was also interest in this standard for use in the SC21 data management export/import project.

The following standards documents use ISO 8211:

- Digital Geographic Information Exchange Standard (DIGEST) (see Section 7.3.1)
- Spatial Data Transfer Specification (SDTS) (US FIPS 173; see Section 7.3.8)
- British Standard Specification for Geographic Information—National Transfer Format (NTF) (see Section 7.3.9)
- International Hydrographic Organization Transfer Format DX-90, SP-57
- Spatial Archive and Interchange Format (SAIF) (for use in Canada)
- Standards being developed by the Japanese Information Center for Science and Technology (JICST)
- Multinational Side-Scan Sonar Distribution (SSS).

ISO 8211 and the standards cited above that are based on ISO 8211 are in wide use. In the United Kingdom, these standards are used by the Ordnance Survey, Military Survey, Hydrographic Office, and Laser-Scan, Inc. US use includes organizations such as the Bureau of the Census, Geological Survey, Defense Mapping Agency (for the ARC Digital Raster Graphics, World Vector Shoreline, and Digital Chart of the World), National Oceanographic and Atmospheric Administration (NOAA) National Charting Division, and Department of the Navy. It is used in software developed for use in most NATO nations.

---

34 Based on [DRA 1994].

A second edition, DIS 8211.2, October 1993, has been developed with changes to provide support for compound arrays (concatenated regular data structures); extended (multi-byte) character sets; better-specified support for simple binary data; fixed point, floating point, and complex binary data; and recursive tree structures in Level 3. The primary negative comment on DIS 8211.2 was that it is poorly structured and uses terminology loosely and inconsistently, so that the technical content might be misunderstood.

7.2 Graphical Data Exchange

Existing military information systems support the generation and display of graphics, a capability that will continue to be required in the future. Graphics are generally not distributed. Instead the underlying data are distributed and the graphics are regenerated at each location where they are needed. In the future the graphics may need to be exchanged. What is needed is a common standard intermediate form in which to transmit graphics, such as exists in other areas of publishing. [Ref. Carlson 1991] Moreover, there is growing interest in using graphics for simulation purposes. [Ref. IDA 1991, p. 152]

Section 7.2.1 describes two standards for exchange of graphical information products: Initial Graphics Exchange Specification (IGES) and the Standard for the Exchange of Product Model Data (STEP, formerly PDES). Standards for graphics interchange services (e.g., Computer Graphics Metafile), Computer Graphics Interface (CGI), the Image Processing and Interchange (IPI) standard, and National Imagery Transmission Format Standard (NITFS) are addressed in Section 7.2.2. Two graphics standards are treated separately in Chapter 8: the Graphics Kernel System (GKS) and the Programmer's Hierarchical Interactive Graphics System (PHIGS).

7.2.1 Graphical Information Product Exchange

7.2.1.1 IGES

The IGES, Version 4.0, is an ANSI standard (*Digital Representation for Communication of Product Definition Data*, Y14.26M-1989) developed by the American Society for Mechanical Engineers (ASME). It is based on the work of the IGES/PDES Organization, which is chaired by NIST. This group establishes information structures to be used for the (1) digital representation and communication of product definition data and (2) representation and transfer of vector graphics data used by various Computer Aided Design and Computer Aided Manufacturing (CAD/CAM) systems. IGES Version 5.1 has been released and Version 6.0 will be processed as an ANSI standard. [Ref. APP 1992] FIPS 177, *Initial Graphics Exchange Specification (IGES)*, based on ASME/ANSI Y14.26M-1989, was issued in November 1992.

MIL-D-28000A, *Digital Representation for Communication of Product Data: IGES Application Subsets*, February 1992, identifies the requirements to be met when product definition data are delivered in the digital format of IGES as specified by ANSI standard Y14.26M. MIL-D-28000A is designed to be incorporated into a contract to define the technical requirements to be met when purchasing product definition data or product data in digital form. The concept of product definition data is defined in MIL-D-28000A as:

> *. . . the totality of data elements required to completely define a product. Product definition data includes geometry, topology, relationship, tolerances, attributes and features necessary to completely define a component part or an assembly of parts for the purpose of design, analysis, manufacture, test, and inspection.*

The specification defines product data as "all data elements necessary to define the geometry, the function, and the behavior of a piece part or an assembly of parts over its entire life span."

MIL-D-28000A defines the technical requirements for the exchange of digital product data in specific application subsets. These subsets are technical illustrations, engineering drawings, and electrical/electronic applications. The technical illustration subset addresses entities that support the exchange of figures and illustrations normally found in a technical publication. The emphasis is on visual clarity for human interpretation. The engineering drawings subset is used to encode product data being acquired in accordance with DoD-D-1000 (*Engineering Drawings and Associate Lists*) for delivery in digital form. Exchange emphasis is on completeness, visual equivalency for human interpretation, and functionality of the received drawing model. The electrical/electronic applications subset addresses the representation and exchange of electrical and electronic products including printed wiring boards, printed wiring assemblies, hybrid micro-assemblies, cables, and wiring harnesses. Emphasis is on component and circuit element descriptions, their placement, their connectivity, and the routing of electrical paths.

NIST is evaluating test tools for IGES Testing and expects a test service to be available in 1993 [Ref. Cugini 1992]. One commercial conformance testing service offered for IGES is located at the CAD-CAM Data Exchange Technical Centre (CADDETC) in the UK [Ref. CALS 1992]

7.2.1.2 STEP

An alternative to IGES for product data interchange is STEP, which is being developed by ISO (CD 10303). STEP was previously known as PDES, but the name was changed to differentiate it from the IGES/PDES Organization (IPO), a voluntary organization of more than 550 American industrial, governmental, and academic entities, which began work on STEP in mid-1984. In April 1988, several major technology companies were incorporated as PDES, Inc., an international consortium dedicated to accelerating the development and adoption of the STEP standard. [Ref. PDES n.d.]

STEP is in the draft stage and may undergo revision at any time. The first version of STEP was scheduled to reach DIS status in December 1992. [Ref. Bloom 1992] ISO standardization is expected in 1994. [Ref. APP 1992] *EXPRESS*, Part 11 of the STEP standard (CD 10303), is an object-flavored information modelling language that has been developed to enable a formal specification of STEP. It is rapidly becoming the language of choice for the formal specification of other data exchange standards, especially in the electronics area. Currently, the language has two forms: (1) EXPRESS itself, a computer processable lexical language, and (2) EXPRESS-G, a graphical subset of the lexical form developed to enable a visually-oriented display of information models. A third form, EXPRESS-I is in development as an instantiation language for data models based on EXPRESS-defined information models. [Ref. Rensselaer 1992]

Since STEP is not being built on an established technology with existing implementations, "validating" the standard is necessary before its adoption. The National PDES Testbed (NPT), located at NIST, was established in 1990 to do this. It is developing a system for testing and evaluating the application protocols, specifying and validating at least one application protocol defined in STEP, and developing a conformance testing system and an institutional framework for validation to be used to test commercial STEP implementations and certify that they comply with the standard application protocol. [Ref. CALS 1992]

7.2.2 Standards for Graphics Services

This section reviews the Computer Graphics Reference Model, Computer Graphics Metafile (CGM), and Computer Graphics Interface (CGI). Chapter 8 reviews other graphics service standards, including the Graphical Kernel System (GKS) (see Section 8.2) and the Programmer's Hierarchical Interactive Graphics System (PHIGS) (see Section 8.3).

7.2.2.1 Computer Graphics Reference Model

The *Reference Model for Computer Graphics* (ISO 11072) defines a basic architecture and consistent terminology for computer graphics. It addresses environment; primitives; geometry, attributes, and aspects of primitives; pictures; collections; metafiles; and archives. There are four environments: application (to which an application interfaces), virtual, logical, and physical (to which the user interfaces). [Ref. RM 1989]

7.2.2.2 Computer Graphics Metafile (CGM)

CGM standards provide a file format suitable for the storage and retrieval of picture information. The file format consists of a set of elements that can be used to describe pictures in a way that is compatible between systems of different architectures and devices of differing capabilities and design. ISO 8632 is a standard for producing a CGM in order to:

- Allow picture information to be stored in an organized way on a graphical software system
- Facilitate transfer of picture information between different graphical software systems
- Enable picture information to be transferred between graphical devices
- Enable picture information to be transferred between different computer graphics installations.

The CGM standards are:

- ISO 8632-1, *Functional Specification*
- ISO 8632-2, *Character Encoding*
- ISO 8632-3, *Binary Encoding*
- ISO 8632-4, *Clear Text Encoding*.

Vendors commonly use CGM as an exchange format for the storage, interchange, or output of a wide range of graphical pictures and numerous CGM implementations exist for use in federal procurements. Virtually all major microcomputer software products can generate and/or interpret CGM files. Moreover, most CGM implementations conform to the CALS Application Profile. CGM is considered to be mature and stable. [Ref. APP 1991, p. 37-38]

MIL-D-28003A, *Digital Representation for Communication of Illustration Data: CGM Application Profile*, November 1991, defines use of the CGM for two-dimensional vector (line segment) picture descriptions or illustrations in technical manuals. Whereas IGES has its principal use within computer-aided design, CGM is becoming widely available for authoring and graphic art workstations. [Ref. CALS/CE 1992]

A CGM test service was launched by NIST in May 1991. The service, analyzes a CGM file to see if it meets requirements that allow the transfer of pictures among different graphical software systems, graphical devices, and computer graphics installation. The File Conformance Test Service tests for conformance to FIPS 128, *Computer Graphics Metafile*, and MIL-D-28003A, *CALS Application Profile*, December 1988. Additionally a test service for CGM

Generator Conformance is being beta tested. NIST is designing the test for an Interpreter Testing Service. [Ref. Cugini 1992]

7.2.2.3 Computer Graphics Interface (CGI)

ISO and ANSI have drafted the CGI standard, formerly the Computer Graphics Virtual Device Interface (CG-VDI), to provide a standard specification of the control and data interchange between device-independent graphics software and one or more device drivers by defining an interface to a virtual graphics device. Device dependencies are allowed in limited circumstances, such as when dealing with raster entities (this is the first graphics standard to contain explicit operations dealing with raster graphics displays). It is designed as a system-level interface to provide efficient device-independent access to graphics devices and processes, but it provides little error checking or error handling. Character, binary, and clear-text codings are provided. This functional specification is also supported by language bindings that specify the exact name for each operation, its parameter sequence, and data types for the parameters.

The ISO/IEC approach to defining a CGI is provided in ISO/IEC 9637, *Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - CGI Data Stream Encoding*. The standard comprises three parts:

- DIS 9637-1 (Part 1): *Character Encoding*
- ISO/IEC 9637-2 (Part 2): *Binary Encoding*
- DIS 9637-3 (Part 3): *Clear Text Encoding.*

The governing CGI standard is ISO/IEC 9636, *Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI)*, which has the following parts:

- ISO/IEC 9636-1 (Part 1): *Overview, Profiles, and Conformance*
- ISO/IEC 9636-2 (Part 2): *Control, Negotiation, and Errors*
- ISO/IEC 9636-3 (Part 3): *Output and Attributes*
- ISO/IEC 9636-4 (Part 4): *Segmentation*
- ISO/IEC 9636-5 (Part 5): *Input and Echoing*
- ISO/IEC 9636-6 (Part 6): *Raster*
- WD 9636-8 (Part 8): *FORTRAN Language Binding of CGI*
- WD 9636-11 (Part 11): *C Language Binding of CGI.*

DIS 9638, *CGI Language Bindings*, has the following parts:

- DIS 9638-1 (Part 1): *FORTRAN*
- DIS 9638-2 (Part 2): *Pascal*
- DIS 9638-3 (Part 3): *Ada*
- DIS 9638-4 (Part 4): *C.*

NIST is monitoring conformance tests being developed for CGI by the European Community. [Ref. Cugini 1992]

7.2.2.4 Image Processing and Interchange (IPI)

SC24/WG1 is developing an *Image Processing and Interchange (IPI)* standard (DIS 12087). Part 1 establishes the conceptual and architectural definitions of the Common Architecture for Imaging (CAI) of the standard. Part 2 establishes the specification of the application program interface (API) part of the standard, called the Programmer's Imaging Kernel

System (PIKS). Part 3 is the Image Interchange Facility (IIF). [Ref. SC24 N 744 1992] DIS 12087 is intended for use in a wide variety of environments where image data are handled. Table 10 indicates the specific areas included and excluded in the terms of reference of the standard.

DIS 12087 is intended to conform with other international standards developed to handle image data. Such standards include the Joint Bi-Level Imaging Group (JBIG) [ISO/IEC 11544] and Joint Photographic Experts Group JPEG) [ISO/IEC 10918-1] compression standards (see Section 7.4), ASN.1 [ISO 8824:1990] (see Section 9.10.1), and ODA [ISO 8613] (see Section 7.1.1). Aspects of the standard that are concerned with the acquisition and display of image data conform with the Computer Graphics Reference Model [ISO/IEC 11072] and its annexes. Part 3 of this standard uses ASN.1 [ISO 8824:1990] in the definition of the IIF.

Table 10. Scope of DIS 12087 on Image Processing and Interchange

Included in IPI	Excluded from IPI
primitive image manipulations	computer graphics
image enhancement	device control
image restoration	image understanding
image analysis	multimedia
image classification (basic)	communications
standard color models	window systems
image transport	sensor image acquisition
image compression and decompression	image presentation

Source: DIS 12087, 1993.

In a recent liaison to SC21, SC24 noted that further improvements in the Packed Encoding Rules of ASN.1 are desirable for encoding the IPI-IIF (see Section 9.10.2). These improvements should address the encoding of multi-dimensional arrays. [Ref. SC21 N 7643 1993]

7.2.2.5 National Imagery Transmission Format (NITF)

The National Imagery Transmission Format Standard (NITFS) is the standard for formatting digital imagery and imagery-related products and exchanging them between members of the Intelligence Community, the US DoD, and other departments and agencies of the US Government. It ensures interoperability of systems used for formatting, transmitting, receiving, and processing imagery and imagery-related information. The NITFS is in essence the suite of individual standards that includes the following: transmission format, four different types of image bandwidth-compression algorithms, communications protocol, forward error correction, Computer Graphics Metafile, and the *NITFS Handbook*. Over 30 different system configurations have been certified compliant with National Imagery Transmission Format (NITF) Version 1.1. NITFS is in Version 2.0. The key improvement in Version 2.0 is the inclusion of a communications support capability, to enable NITF to be transmitted over tactical circuits. Additionally, improved image compression, forward error correction, and enhanced graphics algorithms were added. The relevant standards and specifications are:

- MIL-HDBK-1300, *National Imagery Transmission Format Standard (NITFS)*, June 1993
- MIL-STD-188-196, *Bi-Level Image Compression for the National Imagery Transmission Format Standard*, June 1993

- MIL-STD-188-197, *Adaptive Recursive Interpolated Differential Pulse Code Modulation (ARIDPCM) Compression Algorithm for the National Imagery Transmission Format Standard*, June 1993
- MIL-STD-198, *Joint Photographic Experts Group (JPEG) Image Compression for National Imagery Transmission Format Standard*, June 1993
- MIL-STD-2045-44500, *Tactical Communications Protocol 2 (TACO2) for National Imagery Transmission Format Standard*, June 1993
- MIL-STD-2301, *Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard*, June 1993
- MIL-STD-2500, *National Imagery Transmission Format (Version 2.0) for the National Imagery Transmission Format Standard*, June 1993.

7.3 Geographical Data Exchange

This section covers standards and standardization activities in geographic information exchange. Digital cartographic and geographic information systems have existed for several years; however, their widespread use has been impeded by difficulties in data collection and the need for information sharing standards. Perhaps the most fundamental distinction between the digital representation of cartographic data and the conventional printed graphic is the need to explicitly and unambiguously code the attributes and spatial relationships among the various data elements. Because of the massive amounts of information that must be stored, data compression is a related topic of interest (see Section 7.4).

Specific information system requirements for the processing and interchange of maps and geographical information include the abilities to [Ref. IDA 1991, p. 157]:

- Display and transfer a working color map between two or more headquarters
- Change map features, post symbols, and have zoom capability
- Receive, store, process, display, and integrate all environmental data.

Requirements for use of geographic information systems (GISs) for command and control are being treated in several international forums. In October 1989, a symposium on GISs was held at the SHAPE Technical Centre in The Hague. This symposium addressed requirements, standards, and implementation aspects of GISs for military application. Examples of digital data that may be required for military use of GISs are [Ref. Baybrook 1990]:

- Electronic maps and tactical terrain data.
- Intelligent spatial data, to include maintaining topological relationships interactively, presenting a feature-based view of the data in which attributes can be easily requested interactively, supporting high-speed interactive queries (for which parallel processors and rule-based software may be required), and maintaining prioritized feature symbolization during creating and editing of feature data.
- Topologically structured vector data to support exchange and display of electronic maps, tactical terrain data, and user-generated queries. Features and attributes of the features are associated with points, lines, and areas. Each geographic element is captured and stored only once, together with attributes and relationships to other elements.
- Intelligence collection, data fusion, and intelligence preparation of the battlefield.
- Battle management, mission planning, tactical maneuver, and interdiction.
- Fire support and close air support.
- Antisubmarine warfare.

Digital cartographic and geographic standards generally address (1) encoding or (2) exchange. Typically they reference one another. Currently, all exchange standards are designed for removable media as opposed to establishing communication protocols for exchanging cartographic and geographic information.

There are four basic types of digital cartographic and geographic data:

(1) Digital elevation data
(2) Digital planimetric data
(3) Digital land use and land cover data, and
(4) Digital geographic names data.

Several United States Geological Survey (USGS) circulars cover these types of data:

- FIPS PUB 70-1, *Specifications for Representation of Geographic Point Location for Information Interchange,* 1986 [USGS Circular 878-B]
- FIPS PUB 103, *Codes for Identification of Hydrologic Units in the United States and the Caribbean Areas,* 1983 [USGS Circular 878-A]
- USGS Circular 895-B, *Digital Elevation Models*
- USGS Circular 895-C, *Digital Line Graphs from 1:24,000 Scale Maps*
- USGS Circular 895-D, *Digital Line Graphs from 1:2,000,000 Scale Maps*
- USGS Circular 895-E, *Land Use and Land Cover Digital Data*
- USGS Circular 895-F, *Geographic Names Information System.*

FIPS PUB 70-1 specifies a uniform format for representing geographic point location data in digital form for purposes of information interchange among data systems. It applies only to the three coordinate systems most widely used in the United States to define the position of a point that may be on, above, or below the earth's surface.

FIPS PUB 103 adopts the set of codes used to identify hydrologic units published in Geological Survey Circular 878-A. These codes identify a hydrologic system that divides the United States and Caribbean outlying areas into 21 major regions. These regions are further subdivided into approximately 2,150 units that delineate river basins having drainage areas usually greater than 700 square miles. The codes provide a standardized base for use by water-resources organizations.

In response to a special study chartered by the US Joint Requirements Oversight Council (JROC), the Defense Mapping Agency (DMA) established a program of standardization in August 1990, the goal of which is to develop a comprehensive suite of standards for exchanging, manipulating, and displaying digital Mapping, Charting, and Geodesy (MC&G) data. The Mapping, Charting and Geodesy Technology (MCGT), standardization area will provide for the compatibility and interoperability of digital MC&G databases supporting a wide variety of simulators, command and control, and weapons systems. [Ref. DMA c1990]

Several US military specifications cover digital geographic information exchange:

- MIL-D-89000, *Digital Terrain Elevation Data (DTED),* 26 February 1990
- MIL-D-89005, *Digital Feature Analysis Data*
- MIL-A-89007, *Arc Digitized Raster Graphics.*

The first of these, MIL-D-89000, defines the requirements within the DMA's DTED database, which supports various weapon and training systems. The purpose of MIL-D-89000 is to assure uniform treatment among all mapping and charting elements engaged in coordinated

production and maintenance of this type of data. The UK MOD has related standards, *Digital Terrain Elevation Data* and *Digital Feature Analysis Data*.

The NATO STANAGs relevant to this area include:

- STANAG 3809, *Digital Terrain Elevation Data Exchange Format*
- STANAG 3985, *Preferred Magnetic Tape Standards for the Exchange of Digital Geographic Information*
- STANAG 3986, *Digital Data File Transmittal Form for Geographic Information.*

7.3.1 Digital Geographic Information Exchange Standard (DIGEST)

The 11-nation[35] Digital Geographical Information Working Group (DGIWG) is working on DIGEST. DIGEST may be submitted to ISO, but no definite plan for this has been identified. The present concern is for magnetic tape exchanges, with electronic communications exchanges possible in the future.

The following are the specifications for DIGEST:

- Part 1, *General Description*, Draft, Edition 1.1, August 1992
- Part 2, *Theoretical Model, Exchange Structure, and Encapsulation Specifications*, Draft, Edition 1.1, August 1992
- Part 3, *Codes, Parameters, and Tags*, Draft, Edition 1.1, August 1992
- Part 4, *Feature and Attribute Coding Catalog (FACC)*, Draft, Edition 1.1, August 1992.

DIGEST is intended for standardizing exchanges of digital geographic data and making compatible the digital data products of the participating nations; the draft of the standard was produced in October 1989. This draft was developed to accommodate the exchange of multiple data sets of different data structures using a single format. DIGEST has two parts. The Generic Standard is supplemented by the Minimum Standards Specifications, which are single-data-structure oriented subsets of the Generic Standard. The generic standard contains the necessary file, record, field, and subfield definition and implementation details to exchange all data structures supported by the standard. Each minimum standard specification is geared towards one particular data structure and serves as the basis for the exchange of data only in that structure. The current standard supports the following [Ref. Schneider 1990]:

- Vector topologically structured data, which includes association of features with individual nodes (e.g., water tower), edges (e.g., two-lane highway with an asphalt surface), faces (e.g., forest of deciduous trees), and collections of features associated to nodes, edges, and faces (e.g., Route 1 for a series of line features or city for a collection of three types of features).
- Color-coded and red-green-blue (RGB) coded raster data:
  - An RGB raster image is a collection of red, green, and blue color bands, which when combined for display purposes form the original color of the source graphic.
  - A color-coded image represents each unique color of a scanned graphic as a series of pixels, which represent the information on the original source graphic that utilized that color.
  - The raster structure supports use of subsets and merged sets.

---

[35] The seven member nations are France, Germany, Italy, the Netherlands, Norway, the United Kingdom, and the United States. The four active observers are Belgium, Canada, Denmark, and Spain.

- The raster structure also supports user-defined parameters to indicate scan direction and row and pixel sequencing, which are required for exchanging data derived from scanners that have different capture methods.

- Feature Attribute Coding Catalog (FACC) for feature identification:
  - Features are associated with spatial coordinates or sets of coordinates.
  - Attributes may be associated with features and may serve to designate width, length, material composition, etc.
  - The initial version of the FACC has 300 feature codes and 125 attribute types with associated values. The FACC includes a recommended attribute set for each feature code.
- Transmittal Header File to describe characteristics of the entire transmittal (e.g., originator, edition of the exchange specification used, number of data sets in the transmittal, and security and release information for the transmittal).
- Header information files to describe global characteristics of each data set being exchanged [e.g., quality (currency, accuracy, and completeness), source, projection type, coordinates of the geographic limits of the data set, data structure type]. Qualities can be associated with features and attributes as well as with data sets.
- ISO media standards [using ISO 9660 for Compact Disk-Read Only Memory (CD-ROM) and ISO 1001 for magnetic tapes].
- Security labeling.
- Format implementation compliant with ISO 8211, *Specification for a Data Descriptive File for Information Interchange*.

Standards for two other data structures are being developed for future versions of DIGEST: matrix (to support exchange of elevation data) and spaghetti vector (to support exchange of non-topological vector data).

DGIWG's position is that DIGEST data should be exchanged between map-producing agencies, such as the Defense Mapping Agency (DMA), and not between operational units. Standards governing exchanges between field systems are the responsibility of the system development organization. This is a traditional view in military systems development organizations and leads to substantial interoperability problems, particularly intra-national. The official position notwithstanding, the DGIWG is encouraging the distribution of DIGEST by its member nations to the widest possible audience, including the military services and civilian users.

7.3.2 Geographic Document Architectures

The Directorate of Cartography at the Canadian National Defence Headquarters has proposed that geographic exchange standards be built on a document architecture similar in scope to ODA (see Section 7.1.1). This architecture would address, as does DIGEST, a range of physical media such as magnetic tape and CD-ROM. It would also address exchange of partial data sets and geographic "document" organizations. Unlike DIGEST, the architecture would not attempt to define the sets of feature codes and attributes, which are seen as dependent on political jurisdiction and intended use. For example, Canada must incorporate more geographic ice feature types in hydrographic charts than many other countries. The proposed architectural concept views the architecture as a vessel that carries various properly labeled containers of information. Specification of the channels for transporting the vessel are left, as with ODA, to OSI or other means outside the scope of the architecture. Encapsulation of data for telecommunications would use ASN.1 (ISO 8824 and 8825) and for physical media interchange by ISO 8211. Coding of the information would use such presentation standards as ASCII or ISO 646 for basic text; ISO 6937,

Supplementary Characters, for accents to the text, other alphabets (e.g., ISO 2375, *Non-Latin Alphabets*), and ISO 9282, *Picture Coding* (see Section 7.4), for pictorial information. [Ref. McKellar 1990]

7.3.3 SIMNET Common Geographic Data Model

The US SIMNET program has developed a geographic data model to integrate such heterogeneous data types as digital terrain models, traditional maps, and satellite and aerial imagery and such specialized tools as digital imagery workstations, GISs, relational DBMSs, and high-performance graphics workstations. The data model was defined using ASN.1, which provides a concise, unambiguous means of specifying abstract data types. The specification, *SIMNET Database Interchange Specification* [Ref. Lang 1989], recasts the specification of the data model into a relational data framework in order to take advantage of relational database management and query capability.

The data model represents features in spatial and non-spatial components that can be further subdivided for separate handling and also reassembled to recover the complete feature description. Entities in SIMNET (and many other GIS applications) are represented as objects. For example, networks are represented as collections of line segments, land cover is represented by polygons, terrain is represented by a triangulated mesh, and modeled objects as collections of points, line segments, and triangles. Classes of these object types (such as a class of tree representations) are generated for use in SIMNET data model. Further, the data model permits the enlargement of classes and addition of new classes of objects. For example, several classes of trees are required for simulation: sets of individual trees, collections of irregular groups of trees, lines of trees, uniformly wooded areas, and generalized surface vegetation.

The spatial model represents the physical aspects, including their visual appearance and the intervisibility of pairs of objects (one hides a part of the other). The spatial model encompasses the geometric description, the location, and the orientation of an object within some spatial frame of reference. The spatial model includes aspects that are expected to change only rarely (e.g., the underlying coordinate system) and the modifications are generally only to enhance the fidelity of the representation or the performance (e.g., through data compression). As in DIGEST, the spatial model is based on points, line segments, and triangles. It also includes tetrahedrons for three-dimensional objects, as well as a standard technique from algebraic topology called simplicial complexes to relate the various geometric elements. In this technique, triangles are 2-simplexes, line segments are 1-simplexes, and the three line segments that make up a triangle are functions of the vertices of the triangle.

The non-spatial aspects for simulation may change during execution of a simulation and are therefore expected to be dynamic. These aspects are treated as attributes of objects as a whole or as a component. Examples are color, weight, power, and composition. [Ref. Lang 1990]

7.3.4 IHO Committee for the Exchange of Digital Data (CEDD)

The International Hydrographic Organization (IHO) is developing standards for the exchange of digital hydrographic information. The work is being done by the CEDD. No world-wide standards have yet emerged from this work. One effort of IHO, called the North Sea Project, is establishing an electronic chart database, testing the contents of this database for electronic chart display systems, and evaluating methods of electronic navigational chart updating. [Ref. Stene 1990]

7.3.5 NATO Geographic Conference

The NATO Geographic Conference meets annually (usually in June) to manage and coordinate digital geographic information production in support of NATO plans. The primary tasks are to [Ref. Matthews 1990]:

- Identify common national and NATO requirements for digital geographic information
- Recommend priorities for international cooperative production
- Recommend outline production responsibilities for national agreement
- Recommend outline rules and procedures for operational geographic support and its coordination.

7.3.6 Digital Chart of the World (DCW)

The DCW is a research and development project of the US DMA to develop, refine, and establish a suite of standards that enable the exchange of spatial data on a variety of exploitation systems. The DCW employs a topologically based vector structure and provides digital representation of land surface information on 30-40 CD-ROMs. The coverage is worldwide and the major source is the 270 maps of the 1:1,000,000-scale Operational Navigation Chart series. The DCW is the forerunner for deployed digital databases derived from DMA's Digital Production System (DPS), which was scheduled to produce 31 standard products. A Map, Chart, and Geodesy Feature Data Exchange structure is being defined to archive and exchange DPS products.

7.3.7 Vector Product Standard (VPS)

This standard has reached a prototype stage. A military standard was expected to have been issued in early 1991 but has not been finalized. Although the draft standard has been distributed to the civilian community, there are currently no plans to offer VPS as a civilian standard.

7.3.8 Spatial Data Transfer Specification (SDTS)

The United States National Committee for Digital Cartographic Standards, a multi-agency working group headed by the USGS, which is responsible for most of the US non-military geographic information exchange standards, has issued SDTS. The DMA was an original participant in the development of this standard, but dropped out in favor of its own activities. SDTS has been approved as FIPS 173, effective February 1993. Beginning February 1994, all Federal agencies will be required to use FIPS 173. [Ref. Geo 1992] The USGS is prepared to submit the SDTS to ANSI for promotion as an ANSI standard and then to ISO for promotion as an ISO standard.

The SDTS includes definitions of terminology, a spatial data transfer specification, methods for reporting digital cartographic data quality, and topographic and hydrographic entity terms and definitions. The standard will allow users to transfer digital spatial data sets in a variety of formats between dissimilar computing systems. To support the SDTS, the USGS will coordinate the development of a suite of software tools to assist users in interfacing with the standard. These tools will include the capability to encode and decode the standard from user-specified data models and formats and to encode and decode SDTS data sets to ISO 8211 *(Specification for a Data Descriptive File for Information Interchange)*. [Ref. McDermott 1991]

Version 2 of 8211 reached DIS status in January 1993. It has been produced in response to the need for a mechanism to allow data structures to be easily moved from one computer system to another, independent of architecture. The standard specifies medium-independent and system-

independent file and data record formats for the interchange of information between computer systems.

Other standards under development by USGS include:

- Aquifer names and geologic unit codes
- Classification of wetlands and wildlife services
- EPA (Environmental Protection Agency) parameter codes
- Codes for taxonomic identification of flora and fauna
- Land use and land cover codes
- Public land survey codes
- Cartographic attribute/feature codes.

7.3.9 British Standard Specification for Geographic Information

Draft British Standard BRDF, *British Standard Specification for Geographic Information—National Transfer Format (NTF)*, is a standard for the exchange of digital map data between organizations. The NTF is designed for all types of raster/grid and vector map data. The specification defines media-independent file and data record descriptions for information exchange; description of data elements, vectors, and arrays containing character strings and numeric forms; relationships between data elements; and volume and header information that enables data interchange to occur with minimal specific external description. BSI 91/65602, dated July 1991, is in Release 1.2. It is being developed by the British Standards Institute Technical Committee 36, a committee on geographic information that was set up in 1991 within the Association of Geographic Information which is acting as Secretariat.

7.3.10 Emerging Cartographic Standards for Simulation

A derivative of the SIMNET Common Geographic Data Model, the Project 2851 Standard Simulation Data Base (SSDB) offers improvement over the SIMNET Data Base (see Section 7.3.3), DTED, Digital Feature Analysis Data (DFAD), Interim Terrain Data (ITD), and DIGEST (see Section 7.3.1). SSDB incorporates data types from DTED, DFAD, and ITD, serving as a superset. Terrain; culture information such as slope, vegetation, surface materials, surface drainage, transportation, and obstacles; polygonal and Computer Scene Generation (CSG) models; and raster texture images are included. This tri-service project has two possible formats: SSDB Interchange Format (SIF) and Generic Transformed Database Format (GTDF); both can be derived from SSDB. The SIF format can be used for input to or output from SSDB; GTDF is used only for output to local data bases for image generation. SIF is currently in draft form as a new military standard and is the format of choice for Distributed Interactive Simulation (see IEEE P1278-1993), the replacement for SIMNET.

While SIF seems to require more data than other standards, it has more capabilities. DIGEST is similar to DMA DTED and DFAD. It offers no support for models or levels of detail (LOD). The SIMNET Database Interchange Specification does not support terrain grid data, geo-specific texture, and its format is not easily extended. The Spatial Data Transfer Specification (SDTS) (see Section 7.3.8) developed by the USGS is still in a development stage and as of March 1992, the USGS did not plan to support models. The DMA Vector Product Format (VPF) does not support models, texture or gridded data. The Air Force is developing a new Common Mapping Standard, a mix of old and emerging formats stored as WGS-84 data which are not harmonized.

The US Geospatial Standards Management Committee was formed in 1993. Consisting of representatives from the Services, CINCs, and agencies and chaired by DMA, it provides the management structure for all geospatial-related standards in the DoD.

7.4 Data and Image Compression

An area closely related to map and geographic information is data compression since maps require large quantities of data. For example, at a scale of 1:1,000,000, a digitized map of the world requires 30 CD-ROMs. The Army requires maps that are 1:250,000 and 1:50,000. The use of data compression is not limited to maps however, as the use of complex computer graphics proliferates in areas such as desktop publishing, engineering, and industrial design. Individual manufacturers, software developers, and computer services have adopted their own internal storage formats and data compression algorithms. What is needed is a unifying standard. [Ref. Carlson 1991]

Some of the available image storage standards and commercial software implementations of data compression schemes include [Ref. Carlson 1991]:

- Utah RLE (Run Length Encoding) - University of Utah
- TIFF (Tag Image File Format) - Aldus and Microsoft
- PICT Version 2 (Macintosh) - Apple
- IFF (Interchange File Format) - Electronic Arts
- GIF (Graphics Interchange Format) - CompuServe
- TGA (Targa Image Format) - Truevision, Inc.
- Sun Rasterfile - Sun
- GKS (treated separately as a graphics standard; see Section 8.2)
- CGI (see Section 7.2.2.3)
- ITU-TS Recommendation T.4 (facsimile transmission)
- ISO 11558, *Information Technology, Data Compression for Information Interchange, Adaptive Coding with Embedded Dictionary, DCLZ Algorithm*, 1992.

7.4.1 Joint Photographic Experts Group (JPEG)

Joint Photographic Experts Group (JPEG) is a joint project of IEC/ISO and ITU-TS, which has issued an international standard referred to as the JPEG standard (ISO 10918). The JPEG standard was originally conceived as a companion standard to Group 3 and 4 facsimile standards covering compression and decompression of still-frame, continuous-tone, photographic (gray scale or color) digitized images. The standard comprises two parts. The first part specifies four modes of operation, the different codes specified for those modes, and the interchange format. It also contains implementation guidelines. Several vendors have already introduced JPEG-compatible products. [Ref. Haber 1991] A second standard that deals with still pictures, JBIG (Joint Bi-Level Imaging Group), is also under development.

JPEG's interest in data compression stems from a desire to transmit digital representations of photographs by facsimile. To achieve the desired levels of quality for both color and black and white requires large amounts of data and transmission time. The MPEG is looking at data compression techniques for motion pictures, reducing the data needed to represent each frame, and taking advantage of the redundancy from one frame to the next.

Digital Compression and Coding of Continuous-Tone Still Images (ISO/IEC 10918) has the following parts:

- ISO/IEC 10918-1 (Part 1): *Requirements and Guidelines*, 1993
- DIS 10918-2 (Part 2): *Compliance Testing*, 1993 (IS status expected March 1994)
- WD 10918-3 (Part 3): *Extensions*, 1993 (CD status expected December 1994, DIS in April 1995, and IS in 1996).

7.4.2 Joint Bi-Level Imaging Group (JBIG)

The JBIG standard, *Coded Representation of Bi-level and Limited Bits-per-pixel Still Pictures* [ISO/IEC 11544], will be used to compress bi-level images such as black-and-white photos or pages of text. While pixels can be eliminated without the loss being perceived in the continuous-tone images that JPEG deals with, JBIG deals with simpler images where there can be no image distortion. The American National Standard for JBIG is ANSI/AIIM MS53-1993 entitled *File Format for Storage and Exchange of Images - Bi-Level Image File Format: Part 1.* This standard defines a format for a file containing one page with one image. Page sizes and image sizes can be specified. Both definite length and indefinite length are supported. Clipping of the image can be specified. Image coding may be according to ITU-TS Recommendation T.4 on facsimile. Addition of JPEG image coding will be in a second part of the standard. There are not yet any JBIG implementations. [Ref. Haber 1991] A third standard for video compression has been developed by the Moving Picture Experts Group (MPEG).

7.4.3 Moving Picture Experts Group (MPEG)

ISO/IEC JTC1 SC2/WG11 committee work on MPEG (ISO/IEC 11172) began in 1988 with the goal of achieving a standard by 1990. The parts of ISO/IEC 11172, *Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s*, are as follows [Ref. LeGall 1991]:

- ISO/IEC 11172-1 (Part 1): *Systems*, August 1993—addresses synchronization and multiplexing of multiple compressed audio and video bit streams
- ISO/IEC 11172-2 (Part 2): *Video*, August 1993—addresses compression of video signals at 1.5 Mbits
- ISO/IEC 11172-3 (Part 3): *Audio*, August 1993—addresses compression of digital audio signals at rates of 64, 128, and 192 kbit/s per channel
- CD 11172-4 (Part 4): *Conformance Testing*, November 1993 (DIS expected March 1994, IS in November 1994)
- WD 11172-5 (Part 5): *Technical Report on Software for ISO/IEC 11172*, 1993 (CD expected March 1994, DIS in July 1994, and IS in March 1995).

Another standard with similar scope to MPEG is CD 13818, *Generic Coding of Moving Pictures and Associated Audio Information*, with the following parts:

- CD 13818-1 (Part 1): *Systems*, SC29/WG11, November 1993 [SC29 N 634] (DIS expected March 1994, IS in November 1994]
- CD 13818-2 (Part 2): *Video*, SC29/WG11, November 1993 [SC29 N 634] (DIS expected March 1994, IS in November 1994]
- CD 13818-3 (Part 3): *Audio*, SC29/WG11, November 1993 [SC29 N 635] (DIS expected March 1994, IS in November 1994]
- WD 13818-4 (Part 4): *Conformance Testing*, SC29/WG11, November 1993 [SC29 N 636] (CD expected November 1994, DIS in March 1995, IS in November 1995]

- WD 13818-5 (Part 5): *Technical Report on Software for ISO/IEC 13818*, SC29/WG11 (WD expected July 1994, CD in November 1994, DIS in March 1995, IS in November 1995]
- WD 13818-6 (Part 6): *System Extensions*, SC29/WG11 (WD expected November 1994, CD in March 1995, DIS in November 1995, IS in July 1996]
- WD 13818-7 (Part 7): *Audio Extensions*, SC29/WG11 (WD expected November 1996, CD in March 1997, DIS in July 1997, IS in March 1998]

7.4.4 Digital Video Interactive (DVI)

Digital Video Interactive (DVI) uses a proprietary compression scheme that is backed by Intel Corporation, IBM, and AT&T. IBM and Intel are already marketing DVI products for personal computers, and it has the potential to become a de facto standard.

7.4.5 Other Activities for Data and Image Compression

Section 7.7 describes the MHEG standard, *Coded Representation of Multimedia and Hypermedia Information Objects*, CD 13522.

PIK Reference Model for Image Data. ANSI X3H3.8 has defined a PIK Reference Model with three components: functional services, object data, and operational models. Functional services are classified according to a layered model, in which the highest layer is the application and the lowest layer is a specific implementation. The horizontal dimension in the model identifies different functionalities present at the same layer. The object data correspond to images as well as non-image data of control or parameters (e.g., look-up table, processing parameters). Operational models group together different methods for building applications. [Ref. RNLA 1994, pp. 158-159]

Adapting Coding. ANSI X3 recently announced the approval of a new project on *Data Compression, Adaptive Coding with Sliding Window for Information Interchange* under the auspices of Technical Committee ANSI X3B5, Digital Magnetic Tape. This standard will represent the minimum requirements for the generation of a compressed encoding of data for the interchange of information between systems and provide an effective encoding that results in the compression of data typical to information processing systems. [Ref. X3 1991k]

PDU Compression. Within ISO, the Presentation Rapporteur Group is considering adding support for compression of protocol data units (PDUs) within the presentation protocol. Options could include compression of the complete presentation PDU, compression of the complete user data parameter of the presentation PDU, or a selectable transformation to be applied to the encoding of an individual presentation data value. [Ref. SC21 N 6985 1992]

Picture Coding. In the United States, ANSI X3, X3L3, Audio/Picture Coding, has responsibility for picture coding. Some relevant ISO standards include:

- ISO 9281, *Identification of Picture Coding Methods*, August 1990:
  - Part 1: *Identification*
  - Part 2: *Procedure for Registration.*
- ISO 9282, *Coded Representation of Pictures:*
  - Part 1: *Encoding Principles for Picture Representation in a 7-bit or 8-bit Environment*, September 1988
  - Part 2: *Encoding Principles for Photographic Images*, May 1992.

New Work Items for SC29. SC29 projects include the following new work items:

- *Image Compression Across Multiple Components* [SC29 N 363] (WD expected November 1995, CD in November 1996, DIS in July 1997, IS in 1998)
- *Lossy/Lossless Coding of Bi-level Images* [SC29 N 364] (WD expected November 1995, CD November 1996, DIS in July 1997, IS in 1998)
- *Compression of Up to 5-D Images* [SC29 N 365] (WD expected November 1995, CD in November 1996, DIS in July 1997, in IS 1998)
- *Lossless Compression of Continuous-Tone Still Pictures* [SC29 N 366] (WD expected November 1995, CD in November 1996, DIS in July 1997, IS in 1998)
- *Very-low Bit Rate Audio-Visual Coding* [SC29 N 367] (in four parts: Systems, Video, Audio, and Conformance Testing; WD expected in November 1996, CD in November 1997, DIS in March 1998, and IS in November 1998)
- *Low-Bit-Rate Audio Coding* [SC29 N 368] (WD expected in November 1995 and CD in November 1997)
- *Coding of Man/Multimedia Service Interface Standardization*
- *Interchange of Compressed Pictures.*

Image Compression Initiatives. The following initiatives are being explored for image compression [Ref. RNLA 1994, pp. 159-160]:

- Wavelets—an image compression approach validated by demonstration. WSQ is a wavelet standard developed in the United States, in which the emphasis is on quality and high compression
- Fractal Compression—gives ultra-high compression ratios on the order of 2500:1 and gives better results for zooming than other techniques. Fractal compression can be done in near-real time but requires powerful workstations.
- X-Image Extension (XIE)—defines an X extension for the imaging domain and includes a selection of several recognized algorithms and techniques for color allocation, compression, dithering, etc.
- Common Mapping Standard (CMS)—a standardized cartographic database structure developed by the US Air Force for mission planning systems, providing high-speed access to data including maps, charts, geodesy, and imagery. CMS requires preprocessing from DMA standard products.
- RADIUS Common Development Environment (RCDE)—part of the Research and Development for Image Understanding Systems (RADIUS) project funded by the US Advanced Research Projects Agency. RDCE is a software environment for the development of image-understanding algorithms.
- ImageCalc—a software tool developed by the Artificial Intelligence Center Perception Group of SRI International. It provides the user with image operators and interactive tools. Its internal image representation efficiently handles manipulation and display of large (4,000 x 4,000-pixel) images. ImageCalc runs on a Lisp machine (Symbolics).

7.5 Video Data Exchange

Future information systems will depend on video technology for multimedia information exchanges, training, and intelligence gathering. Information systems may need to store and transmit such video images to analysts at distributed locations. [Ref. IDA 1991, p. 162]

Most of the standards in this area appear to have come from the television industry, specifically, in the United States, the Society of Motion Picture and Television Engineers

(SMPTE). The International Radio Consultative Committee (CCIR) Recommendation 601, *Encoding Parameters of Digital Televisions for Studios*, was published in 1982.

ITU-TS Recommendation H.261, *Video Coder for Audiovisual Services at px64 kbit/s* (commonly referred to as the px64 standard), is a video coding standard that was approved in December 1990 A slightly modified version was developed by ANSI T1. It is T1.314, *Digital Processing of Video Signals - Video Coder/Decoder for Audiovisual Services at 56 to 1,536 kbit/s*, published in 1991.

The real-time simulation community is currently faced with a tradeoff between standards and high-speed performance when available computing power is inadequate to support standards. MIL-STD-1379D, *Military Training Programs*, also addresses video, as does Multi-Media Extensions to Microsoft's Windows (de facto).

In addition, High Definition Television (HDTV) will require studio, exchange, mission, and display standards. For none of these does a single international standard seem likely. In the United States, the FCC intended to issue HDTV standards in the spring of 1993. The FCC action was delayed, however, to allow competing consortia to reconcile their differences. As of November 1993, an alliance of these consortia had announced key technology specifications for digital HDTV sets of the future. The alliance comprises three teams which previously had embraced four different HDTV systems:

- The Advanced Television Research Consortium of Phillips, Thomson Consumer Electronics, the David Sarnoff Research Center, Compression Labs, and NBC
- The team of Zenith and AT&T
- The General Instrument and Massachusetts Institute of Technology team.

The most difficult issue they settled was agreement on a converter that makes progressive and interlaced scanning formats work in one system. The alliance also settled on a 5.1-channel Dolby AC-3 audio technology for HDTV sound, a video compression system called MPEG-2 (which improves picture quality), and a packetized data transport system that allows the transmission of any combination of video, audio, and data. [Ref. HDTV 1993]

7.6 Audio Exchange Standards

Integrated voice technology is another future information system requirement. Some possible applications include:

- Voice mail
- Multimedia documents for training and maintenance
- Computer-generated speech for "eyes-on" situations. [Ref. IDA 1991, p. 166]

In March 1991, ANSI X3 announced the approval of two new standards projects on Voice Messaging:

- *Voice Messaging over MOTIS ISO 10021* is being developed by Task Group ANSI X3V1.4 as a standard protocol for voice messaging to permit the interchange of information objects effectively between various vendors' message systems.
- *Standard User Interface to Voice Messaging* is being developed by Task Group ANSI X3V1.9 to provide users of voice messaging systems with a consistent mode of interaction in a way that is independent of underlying system implementation. The standard will apply only to touch tone telephones. Alternative interface technologies such as speech recognition or screen-based interfaces are not included.

X3L3 also has a Project on Coded Representation of Audio Information; corresponding work on this topic has been cancelled by ISO JTC1/SC27.

The ITU-TS I-Series recommendations for Integrated Services Digital Network (ISDN) (see Section 9.7.6) seeks to combine audio, video, and data transmission on a single system. Currently, the service is limited to a number of disconnected areas since most of the long distance trunk service has not been converted. [Ref. IDA 1991, p. 166]

The ODA (see Section 7.1.1) is designed to allow for extensions including additional types of content such as sound. In addition, ITU-TS G.721 is a standard audio encoding method.

Standards for coding of moving pictures and associated audio information are discussed in Section 7.4.3 above.

7.7 Multimedia Standards

An issue that transcends audio or video data exchange alone is that of integrating all these nascent standards efforts by developing a framework or reference model for digital multimedia. This problem has only recently been considered by ISO/IEC JTC1. In addition to algorithms, bit streams, encoders, and decoders, both users and application programmers will need complete systems and environments. Open systems are required, each with an interactive multimedia application development/utilization environment, including some or all of the following [Ref. Fox 1991]:

- Multimedia data capture tools
- Multimedia data editors/synthesizers
- Multimedia scripting language tools
- Multimedia data integrator/sequencer tools
- Multimedia database and storage/retrieval layout tools
- User interface development tools
- Simulation, testing, and publishing assistance tools
- Archiving, versioning, backup, and recovery tools
- Project management tools
- Run-time support environment for application use.

Developing a framework is but one suggestion of the ISO/IEC JTC1 Ad Hoc Technical Study Group on Multimedia and Hypermedia. Other tasks include:

- Discussing and recording a procedural plan for establishing multimedia and hypermedia requirements and a procedure for communicating these requirements among the relevant groups within JTC1
- Preparing a report on the general concepts and definitions related to multimedia and hypermedia and trying to reach agreement on general concepts.

SC18 has been given the responsibility for developing the framework. In October 1992, it issued a *Working Draft of the Technical Report on Multimedia and Hypermedia: Model and Framework* [SC21 N 7430, November 1992]. SC18 will work closely with the Multimedia/Hypermedia Experts Group (MHEG) (JTC1 SC29/WG12) in developing the Audio Visual Interactive (AVI) Scriptware work item (JTC1 N 809) as a two-part standard [Ref. JTC1 N 1161 1991]:

- Part 1: *Functional definition*, being the responsibility of SC18
- Part 2: *Encoding*, being the responsibility of SC29.

In 1993, another MHEG standard, *Coded Representation of Multimedia and Hypermedia Information* achieved CD status (CD 13522). Its parts are as follows:

- CD 13522-1 (Part 1): *MHEG Objects Representation - Base Notation (ASN.1)*, 1993 (DIS expected March 1994 and IS in November 1994)
- WD 13522-2 (Part 2): *Alternate Notation (SMSL)*, 1993 (CD expected March 1994, DIS in November 1994, and IS in February 1995)
- WD 13522-3 (Part 3): *MHEG Extensions for Scripting Language Support*, 1993 (CD expected December 1994, DIS in June 1995 and IS in December 1995).

SC24 has an new work item proposal to develop a *Presentation Environment for Multimedia Objects (PREMO)*, November 1992 [SC24 N 847]. PREMO will be a multi-part standard that will address all aspects of the construction of, presentation of, and interaction with multimedia objects. Multimedia objects include computer graphics, moving computer graphics (animation), synthetic graphics of all types, text, audio, still images, moving images (including video), images coming from imaging operations, and any other context type of combination of context types that can be "presented." Target dates are CD in June 1994, DIS in June 1995, and IS in 1996. [Ref. SC21 N 7642 1993]

SC29 has authorized the following new work item: *Coding of Standard Multimedia Scripting Language (SMSL)*, for which WD is expected February 1994, CD in June 1994, DIS in December 1994, and IS in 1995.

In March 1992, ANSI X3 announced the approval of a new project on *Hypermedia and Multimedia Glossary*, an addendum to ANSI X3.172-1990. [Ref. X3 1992f] Another ANSI (X3L3) project is *Coded Representation of Multimedia and Hypermedia Information Objects*, Part 1: *Multimedia Synchronized Objects* and Part 2: *Hypermedia Objects*.

The Interactive Multimedia Association (IMA) has been actively promoting industry-wide compatibility of multimedia products. In 1988, the IMA Compatibility Committee was formed to develop recommendations for multimedia applications that would permit their portability across a variety of hardware-software platforms. *Recommended Practices for Multimedia Portability*, Release R1.1, was published October 1990. It recommends commands for general system services, visual management, videodisc players, and X-Y-input devices. The recommended practices furnish platform independence but not device interoperability.

In November 1990, the DoD incorporated the IMA specification in Appendix D of MIL-STD-1379. In March 1991, the DoD issued DoD I 1322.20, *Development and Management of Interactive Courseware*, which mandates that all interactive multimedia courseware and hardware systems purchased by the DoD must comply with IMA specifications. [Ref. Jurgen 1992]

In August 1993, it was announced that an international group of vendors has set out to promote the design and use of *collaborative* multimedia applications, which use video conferencing and other techniques to allow people who cannot meet face to face to work together from any points on the globe. The seven founding members of the Multimedia Communications Community of Interest, BT, France Telecom, Deutsche Bundespost Telekom, IBM, Intel, Northern Telecom and Telstra, have invited other companies to join. The group will promote applications that let people in different locations view documents, images, graphics, and full-motion videos on a personal computer screen, discuss what they see on the screen, and make changes that all other participants can see. This must be possible regardless of the operating system, computer equipment, or telecommunications company being used. The group will promote the use of

existing industry standards, and, where standards do not exist, will define working specifications. A series of field trials was planned to begin in the first quarter of 1994. [Ref. OSN 1993p] Section 9.11.4.2 also addresses some X.400-related computer conferencing and asynchronous group communication standards work.

7.8 Assessment of Coverage by Standards

Data interchange services establish data formats for interchange of documents, graphics data, and product description data.

In the area of document exchange, standards exist that would fulfill an AIS's requirements. There is evidence that these standards are stabilizing as Document Application Profiles (DAPs) begin to appear. While both ODL and SGML can be used with ODA and information can be transferred between the two formats, there are some advantages to using SGML. Not only does CALS use SGML, but more commercial products are available for it than for ODL. Moreover, it is human-readable, preserves user file divisions, and is extensible to other architectures. It also possesses a broader information processing orientation than does ODL, which is concerned solely with document processing. ODA (ISO 8613:1989) models are still incomplete, and there is still ongoing work on the connection between document logical structure, layout, and content. Gaps in ODA/ODIF standards (for which future ISO work is planned) include: revision collection, status, rationale, and author information; document annotations; automatic content generation of listings such as table of contents, tables of figures, indexes, glossaries, and cross references; business charting; data in documents, such as spreadsheets; exchange of hypertext-based documents; and exchange of documents that include voice and audio information.

Central to CALS is the use of EDI (FIPS 161; EDIFACT, ISO 9735:1988; X.12-1986; ITU-TS X.435:1991) for business data interchange. EDIFACT and X.12 differ in syntax control segments, data segments, and data elements. The various versions of EDI are expected to merge (in a future edition of ISO 9735) and to use X.400-1988 messaging. An argument against using the CALS standard as a model is that it is oriented to technical weapons systems support documentation which may not be appropriate to an information system.

The status of technology in the area of data interchange is such that standards do not yet manage information as a database where content is encoded and structure and form attached.

IGES is suitable for engineering data but does not include all interfaces for use, such as the interface between the data specification and numerically-controlled machining tools. STEP represents complex data objects (e.g., technical diagrams and documents) suitable for product development (e.g., for advanced manufacturing machines) from initial concept design to manufacturing and product support.

Graphics services standards all appear to be stable and mature with a high level of consensus and product availability. However, none address the question of distributed graphics. A common intermediate standard is needed to exchange graphics data stored on different platforms.

The remaining data interchange standards areas (geographic, data compression, video, and audio) are far less stable and mature. A lack of standards has impeded interoperability among digital cartographic and geographic information systems. For example, SDTS (FIPS 173) has been developed for transfer of digital spatial data among heterogeneous computer systems; however, an international forum (with the participation of the US Defense Mapping Agency) has developed an alternative specification, DIGEST. Agreement on such a standard is essential to the

interoperability of geographical information systems (GISs) and between GISs and other information systems (at least to import terrain data and map graphics). An information system proponent will need to monitor standards developments in these areas as well as in the area of multimedia standards where standards are generally lacking. For example, one promising technology that has been crippled by a lack of standards is multimedia mail. [Ref. Borenstein 1991]

Data compression standards, particularly JPEG and MPEG have attracted significant support, but the future has been clouded by other vendors claiming to have substantially improved technical approaches to compression.

8. GRAPHICS SERVICE STANDARDS

Quick Reference	
Topic	Page
Assessment	130
GKS	129
PHIGS	130
Ref Mod Comp Graphics	129

This chapter reviews standards being developed for computer graphics. These include the Computer Graphics Reference Model, the Graphical Kernel System (GKS), and Programmer's Hierarchical Interactive Graphics System (PHIGS). The Computer Graphics Metafile (CGM) and Computer Graphics Interface (CGI) are discussed in Sections 7.2.2.2 and 7.2.2.3, respectively. The Image Processing and Interchange (IPI) standard is discussed in Section 7.2.2.4. An overview of the status of key standards for graphics services is given in Table 11.

8.1 Reference Model for Computer Graphics

As noted in Section 7.2.2.1, the *Reference Model for Computer Graphics* (ISO 11072) defines a basic architecture and consistent terminology for computer graphics. It addresses environment; primitives; geometry, attributes, and aspects of primitives; pictures; collections; metafiles; and archives. There are four environments: application (to which an application interfaces), virtual, logical, and physical (to which the user interfaces). [Ref. RM 1989]

8.2 Graphical Kernel System (GKS)

The GKS standard, ISO 7942 (FIPS 120-1), specifies a language-independent nucleus of a graphics system. For integration into a specific programming language, GKS is embedded in a language-dependent layer obeying the particular conventions of that language. This layer (technically referenced as a "binding") has been defined for the programming language Ada in ISO 8651-3, based on the Ada *Programming Language* (ISO 8652). It has also been defined for the programming languages FORTRAN (ISO 8651-1), Pascal (ISO 8651-2), and C (ISO 8651-4).

GKS is considered to be a mature and stable standard. A full range of products and automated tools based on GKS has been available from various vendors for 5 or more years. However, it is limited to two-dimensional (2D) graphics. [Ref. APP 1991, 41]

A three-dimensional (3D) version of GKS is being developed in ISO. The purpose of GKS-3D is to specify extensions to GKS for defining and viewing 3D wire-frame objects. As such, the GKS-3D documents only describe additions to be made to GKS.

Table 11. Status Overview of Key Graphics Service Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
GKS	●	●	●	●	●	●	●
PHIGS	●	●	●	○	●	●	●

Key: ● High Evaluation; ○ Average Evaluation; Blank Low Evaluation

Source: [Ref. APP 1993]

LOC -- Level of consensus
PAV -- Product availability
CMP -- Completeness
MAT -- Maturity
STB -- Stability
DFU -- De facto usage
PRL -- Problems/limitations

The GKS-3D portions of the GKS standards are:

- ISO 8805, GKS *for Three Dimensions (GKS-3D) Functional Description*, October 1988, and ISO 8805/WDAD 1, Addendum 1: *Name Set Addendum*, April 1987
- DIS 8806-1, *GKS-3D Language Bindings - Part 1: FORTRAN*, November 1988
- DIS 8806-3, *GKS-3D Language Bindings - Part 3: Ada*, 1989
- ISO/IEC 8806-4, *GKS-3D Language Bindings - Part 4: C*, 1991
- ANSI X3.122.5, *GKS-3D Language Bindings - LISP*.

One of the major design goals in ISO is compatibility between GKS-3D and GKS. The 2D primitives of GKS can be seen as a subset of the 3D primitives obtainable via GKS-3D. This allows a GKS-3D program to read both 2D and 3D metafiles (by forcing 2D primitives to the z=0 plane); thus, upwards compatibility is being sought.

A GKS test service is available at NIST. It tests for conformance to FIPS 120-1. NIST distributes an information pack from which the client conducts a pre-validation. NIST then conducts on-site testing and generates a test report. [Ref. Cugini 1992]

8.3 Programmer's Hierarchical Interactive Graphics System (PHIGS)

The standards for PHIGS, include language bindings for graphics interfaces:

- ISO 9592-1, *PHIGS - Part 1: Functional Description*, and ISO 9592-1/AM1: *PHIGS Plus Support*
- ISO 9592-2, *PHIGS - Part 2: Archive File Format*, and ISO 9592-2/AM1: *PHIGS Plus Support*
- ISO 9592-3, *PHIGS - Part 3: Clear-Text Encoding of Archive File*, and ISO 9592-3/AM1: *PHIGS Plus Support*
- ISO 9592-4, *PHIGS - Part 4: PHIGS Plus*
- ISO/IEC 9593-1, *PHIGS Language Bindings - Part 1: FORTRAN Binding*
- DIS 9593-2, *PHIGS Language Bindings - Part 2: Extended Pascal*
- ISO/IEC 9593-3, *PHIGS Language Bindings - Part 3: Ada*
  - DAM 1: *Incorporation of PHIGS Plus*
- ISO/IEC 9593-4, *PHIGS Language Bindings - Part 4: C*, 1991.

PHIGS (FIPS 153) is a full-functioned specification for the development of interactive two- and three-dimensional graphics applications that manage hierarchical database structures containing graphics data. Numerous PHIGS implementations are available for various hardware/software platforms. PHIGS is mature and relatively stable. No changes are planned in the next 1 to 3 years. Bindings for FORTRAN and Ada have been adopted. Bindings for C and Pascal are under development. A new standard, PHIGS Plus (ISO 9592-4) has been developed, which adds shading, lighting, and other advanced graphics programming capabilities that were not included in PHIGS. Conforming PHIGS programs will be able to execute under PHIGS Plus with no change. [Ref. APP 1991, p. 42] PEX is discussed in Section 5.2.5.

A PHIGS test service is available from NIST to test implementation for conformance to FIPS 153. It is currently available for the FORTRAN binding. Version 2 became available on October 1992. [Ref. APP 1992]

8.4 Assessment of Coverage by Standards

Graphics services standards all appear to be stable and mature with a high level of consensus and product availability.

9. NETWORK SERVICE STANDARDS

In general, data communication involves three agents: processes, hosts, and networks. Processes are the fundamental entities that communicate and execute on hosts (computers), which can often support multiple simultaneous processes. Hosts are interconnected by networks, and the data to be exchanged are transmitted by the network from one host to another. [Ref. Stallings 1987, pp. 14-15]

The purpose of this chapter is to identify existing and emerging standards for network services. It documents inter-relationships among interfaces and standards and describes how they can be mixed to provide the desired network services. The chapter is organized as follows:

- OSI Reference Model (9.1)
- Government/military requirements for OSI (9.2)
- Physical Layer standards (9.3)
- Data Link Layer standards (9.4)
- Local area network (LAN) technologies (9.5)
- Broadband technology (9.6)
- Network Layer standards (9.7)
- Transport Layer standards (9.8)
- Session Layer standards (9.9)
- Presentation Layer standards (9.10)
- Application Layer standards (9.11)
- Internetworking (9.12)
- Other standards and issues (9.13)
- Assessment (9.14).

9.1 OSI Reference Model

ISO/IEC has developed a seven-layer model to implement standards for network services. This model, called the Open Systems Interconnection (OSI) Reference Model, provides a common basis for coordinating standards developed for the purpose of system interconnection, while allowing existing standards to be placed into perspective within an overall framework. The term OSI qualifies standards for the exchange of information among systems that are *open* to one another for this purpose by virtue of their mutual use of the applicable standards. The fact that a system is open does not imply any particular system implementation, technology, or means of interconnection, but refers to the mutual recognition and support of the applicable standards. [ISO 7498] This section summarizes the elements of the OSI Reference Model upper and lower layer structures.

Quick Reference

The OSI Reference Model comprises seven functional layers. The application, presentation, session, and transport layers (Layers 7, 6, 5, and 4, respectively) together implement the processing-related functions and are termed the upper layers. The lower layers—network, link, and physical layers (Layers 3, 2, and 1, respectively)—implement the communication-related functions. Two types of standards are defined for each layer: service definition, which abstractly defines the externally visible service provided by the layer; and protocol specification, which defines the interactions that peer entities must carry out in order to provide the requested layer service. The roles and primary standards for each layer are summarized in Table 12. Both ISO/IEC and ITU-TS (X.211-217, X.224-227) standards are cited.

9.1.1 Service Definitions and Protocol Specifications

The major aspects of services and protocols may be described as follows [Ref. Stallings 1993, pp. 30-34]:

- Services. An OSI service definition is a functional description that specifies *what* services are provided but not *how* the services are provided. The details of how the services are provided may differ from one open system to another without loss of interoperability. Thus, the focus is on interfaces between layers without unduly constraining developers on providing (standard) services within each layer. The services between adjacent layers in the OSI architecture are expressed in terms of primitives and parameters. A primitive specifies the function to be performed, and the parameters are used to pass data and control information. The actual form of a primitive (e.g., a procedure call) is implementation dependent.
- Protocols. An OSI protocol is concerned with exchanging streams of data between peer entities. Characterized as consisting of a sequence of blocks of some bounded size, protocol data units (PDUs) contain control information used to coordinate the joint operation of two entities engaged in the protocol. In addition, some of the PDUs contain (encapsulate) user data from the next higher layer. However, data from one layer may be segmented prior to encapsulation by the next lower layer and will therefore need to be reassembled by the peer layer on the receiving system before being passed to the next higher layer in the receiving system. Reasons for segmentation include limitations on block size, efficiency of a smaller PDU size, more equitable access to communications resources, shorter average delay, and use of smaller buffers.

Table 12. Roles and Standards for Services and Protocols of OSI Reference Model

Layer	Role	Service Definition	Protocol Specification
Layer 7 (Application)	Provides services to users of the OSI environment; examples include transaction server, file transfer protocol, and network management; service elements include association control (ACSE), remote transfer (RTSE), and remote operations (ROSE), Transaction Processing User ASE	ACSE: ISO 8649 (X.217) RTSE: ISO 9066-1 (X.218) ROSE: ISO 9072-1 (X.219) TP User ASE: ISO 10026	ACSE: ISO 8650 (X.227) RTSE: ISO 9066-2 (X.228) ROSE: ISO 9072-2 (X.229)
Layer 6 (Presentation)	Performs generally useful transformations on data to provide a standardized application interface and common communications services; examples include encryption, text compression, and reformatting; specifies or, optionally, negotiates the way information is represented for exchange by application entities and provides the representation (syntax not meaning) of (1) data transferred between application entities, (2) the data structure that the application entities use, and (3) operations on the data's structure	ISO 8822 (X.216)	ISO 8823 (X.226)
Layer 5 (Session)	Provides the control structure for communication between applications; establishes, manages, and terminates connections (sessions) between cooperating applications; allows cooperating applications to organize and synchronize conversation and to manage data exchange; session services are used during a session to regulate dialogue by ensuring orderly message exchange on the session connection	ISO 8326 (X.215)	ISO 8327 (X.225)
Layer 4 (Transport)	Provides reliable, transparent transfer of data between end points (cooperating session entities); provides end-to-end error recovery and flow control	ISO 8072 (X.214)	ISO 8073 (X.224)
Layer 3 (Network)	Provides upper layers with independence from the data transmission and switching technologies used to connect systems; is responsible for establishing, maintaining, and terminating connections across networks; provides packet routing and relaying between end systems on the same network or on interconnected networks; provides hop-by-hop network service enhancements, flow control, and load leveling; services are independent of the distance separating interconnected networks	ISO 8348 (X.213)	Described in separate figure (see Section 9.1.3)
Layer 2 (Data Link)	Provides communication between two or more adjacent systems; provides for the reliable transfer of data across the physical link; sends blocks of data (frames) with the necessary synchronization, error control, and flow control	ISO 8886 (X.212)	
Layer 1 (Physical)	Provides a physical connection for transmission of data between data link entities; is concerned with the transmission of an unstructured bit stream over a physical link; involves such parameters as signal voltage swing and bit duration; deals with the mechanical, electrical (e.g., electrical coding and decoding), and procedural characteristics to establish, maintain, and deactivate the physical link	ISO 10022 (X.211)	

Sources: [Stallings 1993, pp. 25-36], [IGOSS 1993, pp. 11-12].

9.1.2 Status of OSI Reference Model Standards

Developed in 1977 and initially published by ISO in 1979, the OSI *Basic Reference Model* became an ISO standard (ISO 7498) in October 1984. ISO JTC1/SC21 has a standing document (SD-9), *Approved Commentaries on the Basic Reference Model for Open Systems Interconnection*, last updated in December 1993 [SC21 N 8342]. The following extensions have been added or are in progress [Ref. Tang 1992, pp. 17-18]:

- ISO 7498 AD 1, *Connectionless Mode*. The original OSI model was connection-oriented, meaning that the communicating parties have to establish a logical connection before communication can take place. However, there is a demand for connectionless mode communication in LANs, network management, and interactive environments. ISO/IEC 7498-1:1994 (*Basic Reference Model*, Part 1: *General Aspects*) incorporates this addendum. This revision addresses upper and lower layers, and it permits routing and relaying between individual local networks in the Data Link Layer. It also clarifies the distinction between connectionless and connection-mode operation, aligns the service definitions for the lower and also upper layers, improves consistency of layer descriptions, adds Reset as a facility to the Data Link Layer, adds Suspend and Resume as functions in the Transport Layer, and aligns this work with ITU-TS (X.200).
- ISO/IEC 7498-1:1994, *Basic Reference Model*. This part is a new edition of ISO 7498 that creates a multi-part standard and incorporates AD 1. IS text was available in November 1993 but ITU-TS approval is not yet complete (balloting ended February 1994).
- ISO 7498-2, *Security Architecture*, February 1989. This part defines OSI security architecture as an enhancement to the OSI architecture. It describes security architectural concepts such as security services and security mechanisms. It also outlines how security services can be placed in the OSI Reference Model. SC21 proposed confirmation (continuance as a valid standard without revision) of this part in June 1993.
- ISO 7498-3, *Naming and Addressing*, March 1989. This part defines a general mechanism for the use of names and addresses to identify and locate objects in an OSI environment (OSIE). SC21 has proposed a revision incorporating new work (Q1/68 an Q1/70) on naming and addressing.
- ISO/IEC 7498-4, *Management Framework*, November 1989. This part defines a framework for management activities pertinent to OSI and management services supported by the OSI management protocols. It covers the management concepts, management functional areas, and management structure. In June 1993, SC21 proposed confirmation of this standard with the addition of a technical corrigendum currently in the form of a defect report [SC21 N 6658].
- WD 7498-5, *Architecture for Multi-Peer Communications*. This work is a reactivation of earlier work conducted as ISO 7498 PDAD 2 on Multi-Peer Data Transmission (MPDT), which was suspended in November 1989. It will address requirements such as multi-endpoint connection (see Section 9.2.2). Balloting on the new work item proposal was successfully completed in November 1993, and a CD is expected in 1996.

Related Models. The *Basic Reference Model* is being supplemented by a number of other models and frameworks within the context of OSI. These include *Application Layer Structure* (ISO/IEC 9545), *Internal Organization of the Network Layer* (ISO 8648), *Management Information Model* (ISO/IEC 10165-1), *Upper Layer Security Model* (ISO/IEC 10745), *Remote Procedure Call Model* (DIS 11578-1), *Generic Upper Layers Security (GULS) Overview, Models and Notation* (DIS 11586-1), *Transaction Processing Model* (ISO 10026-1), and *Remote Operations Model* (CD 13712-1).

Naming and Addressing. TR 10730, *Tutorial on Naming and Addressing*, introduces the main concepts and mechanisms that are defined in ISO 7498-3 to fulfill the needs for naming and addressing objects in the OSI environment. It also includes the rationale for some of the important decisions made in the naming and addressing architecture. An amendment, TR 10730

WDAM 1, *Directory Names*, is in progress but is dependent on progression of an amendment to ISO/IEC 9834-1 on registration authorities (see Section 12.3). In addition, SC21/WG1 proposed in May 1992 a new question (Q1/68) on the definition of the term *application-process-title*. This term is introduced in ISO 7498-3, but not formally defined. A need has arisen to reference such a definition from ISO 9834-6. The definition that was proposed was "a name that is used to identify unambiguously an application-process" [Ref. SC21 N 7094 1992]. ISO 7498-3 is being revised to include Q1/68.

Two documents are maintained as references on standard definitions for OSI vocabulary. SC21 has an internal document, *Collections of Definitions of OSI Vocabulary*, last updated in July 1992 [SC21 N 7268]. A formal standard developed by JTC1/SC1 is DIS 2382-26, *Vocabulary*, Part 26: *Open Systems Architecture*, January 1992.

In January 1992, the Conference of NATO Armaments Directors (CNAD), upon the recommendation of the NATO Communications and Information Systems Committee (NACISC), designated the NATO Integrated Communications System Central Operational Authority (NICS COA) as the NATO OSI Registration Authority for naming and addressing. [Ref. CNAD 1992; NACISC 1992a]

Related Standards. SC21 has developed guidance for users and definers of service standards. The initial work was released as a technical report, ISO/TR 8509, *Service Conventions*, September 1987. A more comprehensive standard to replace the technical report is ISO/IEC 10731, *Conventions for the Definition of OSI Services*, 1993 (ITU-TS ballot closed in November 1993). ISO 10731 consists of three parts: *General Model and Conventions*, *Application Layer*, and *Layers 1-6*.

Several architecture-related topics are discussed elsewhere. As noted, security is addressed in Section 11.2, quality of service (QoS) and OSI management in Section 12.1, and formal description techniques (FDTs) and conformance testing in Section 12.2. Open system environments are discussed in Section 15.1.3 and 15.3, and application programming interfaces (APIs) are treated in Section 15.2. International standardized profiles (ISPs) are discussed in Section 16.1.2.

9.1.3 Overview of OSI Base Standards

Figure 6 provides an overview of the standards applicable to each layer of the OSI Reference Model. The layer OSI standards are connected by vertical lines to depict a wide range of stacks for application (upper layer) and transport (lower layer) options. Security is covered in Chapter 11; and registration authorities, conformance testing, and other standards applicable to all the classes of services are identified and discussed in Chapter 12—these are not included in Figure 6.

The types of transfer service options are identified along the bottom of Figure 6. Standards and options in a layer common to several stacks are shown in blocks. For example, the Logical Link Control (LLC) in Layer 2 is common to stacks for all types of LANs shown in Figure 6. Above the LLC, the CO-mode X.25 Packet Level Protocol (PLP, ISO 8208, 8878, 8880-1, 8880-2, and 8881), and the connectionless network protocol (CLNP) apply to each of the four LAN options. The X.25 PLP (ISO 8208 and 8878) in Layer 3 and the High-Level Data Link Control (HDLC) in Layer 2 are required for the stacks for four types of circuits: Circuit Switched Data Network (CSDN), Packet Switched Data Network (PSDN), Point-to-Point Subnetwork, and Switched Telephone Network (STN).

Appendixes D and E provide a complete list of OSI (and other) standards developed by ISO/IEC and ITU-TS. Appendix D is organized by layer of the OSI Reference Model and contains brief titles, whereas Appendix E is a numerical listing that contains full titles, dates, and comments on anticipated completion of draft documents.

9.1.4 Connection Orientation for OSI

One of the important issues that must be considered when reviewing OSI standards is the choice between connection-oriented (CO) services (also called "virtual circuit" services) and connectionless-mode (CL) services (also called "datagram" services). Each of the seven OSI layers, except the Physical Layer, may be CO or CL. (The Physical Layer has no connection orientation.) The OSI Reference Model recommends that the upper four layers be either all CO or all CL. The following paragraphs, based on [Ref. Purton 1987; Stallings 1985, 1987a, and 1993; and NATO 1987], address some prominent distinctions between these two classes of services.

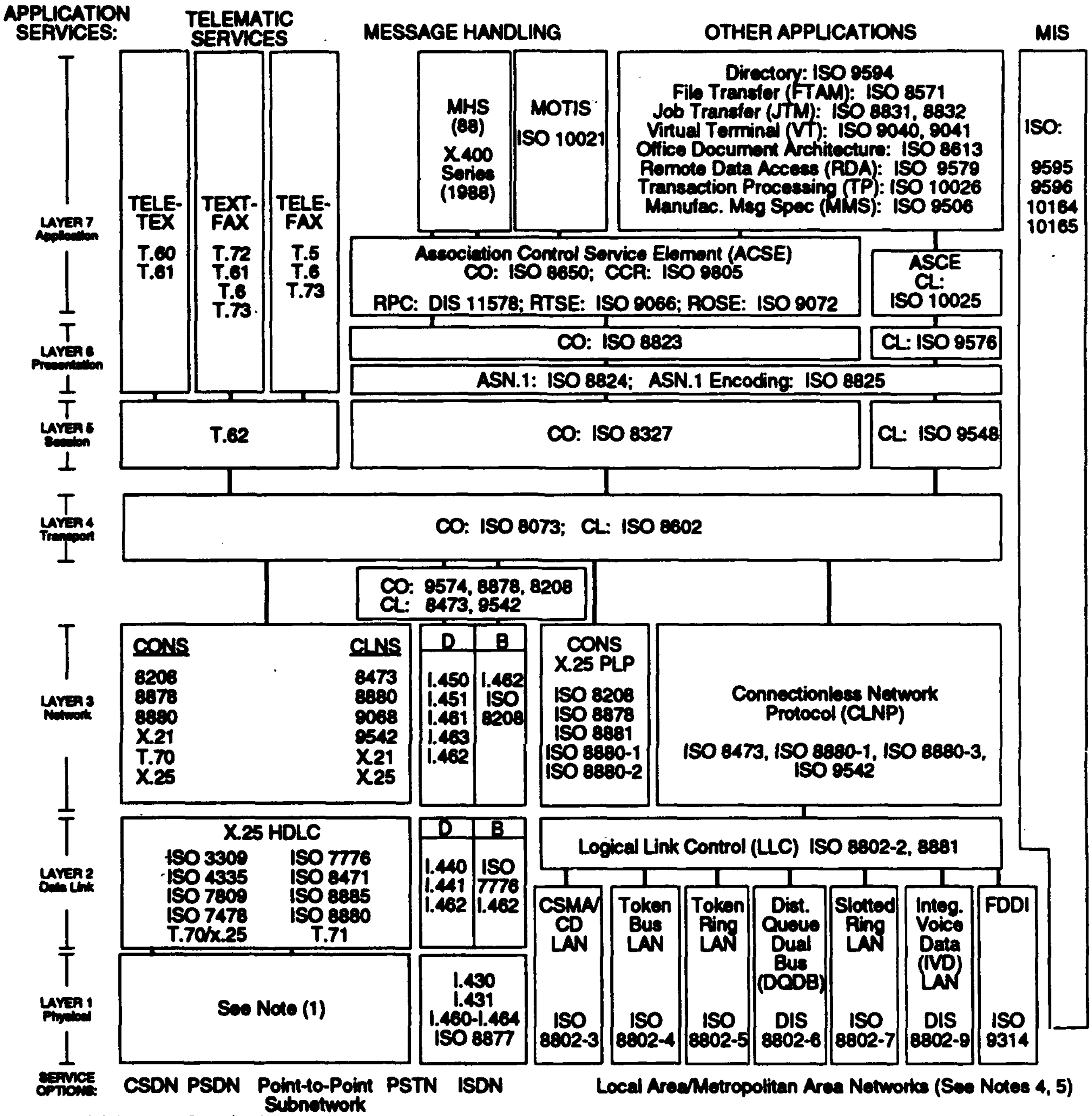
With connection-mode transmission, a logical connection is set up between peer entities prior to the exchange of data. This connection allows both sides to maintain state information about the history and current status of the transmission of protocol data units between the two sides. In CL operation, each data unit transmitted is independent of previous or subsequent data units, and no connection is set up. Table 13 contrasts the characteristics of the two modes. [Ref. Stallings 1993, p. 41]

Table 13. Characteristics of Connection-Mode and Connectionless-Mode Data Transmission

Connection-Mode Transmission	Connectionless-Mode Transmission
Clearly distinguishable lifetime	Single-access service
Three-party agreement	Two-party agreement
Negotiation and renegotiation	No negotiation
Connection identifiers	Self-contained data units with service access points
Data-unit relationship	Data-unit independence

Source: [Stallings 1993, p. 41].

The basic difference between CO and CL service is that CO service requires that an explicit relationship be established between the interacting peer entities before any further activity can take place, while in CL service no such explicit relationship occurs. A connection preserves the state of peer-to-peer communications from one data transfer to the next, storing and distributing information regarding the connection within the service provider, while the CL transmission does not. In CO service the relationship may be real—such as a dedicated circuit—or virtual, such as a particular path from node to node between peer entities in a CO packet-switched service. In the latter case the path would be agreed upon before data transfer begins and would remain unchanged during the transfer. A heuristic example of CO service is any national public telephone service; the regular delivery postal service is a heuristic example of a CL service.



Notes:

(1) Layer 1 Standards are:
  (a) CSDN/PSDN: V.24, V.28, V.35, V.36, V.37; X.21, X.21bis, X.22, X.24, X.26, X.27
  (b) Point-to-Point Subnetwork: Predefined
  (c) PSTN: V.10, V.11, V.20, V.24, V.28, V.31, V.31bis, V.35, V.36, V.37

(2) Standards are ITU-TS unless designated ISO, DIS.
(3) Stacks are based on series 1993 NOSIP Strategy. (JTM, MMS, Token Ring, LAN, and Slotted Ring LAN are omitted from NOSIP).
(4) Each LAN/MAN standard addresses both Layer 1 and Layer 2 Media Access Control (MAC) for Layer 2.
(5) Interworking standards include 10028 (MAC Bridging), and 10028, 10029 (Routing)

Figure 6. Stacks of OSI Base Standards

CO service has three phases: connection establishment (set up), data transfer, and connection release (call termination). The route of each data packet is determined by the state of the network during the call set up and remains static for the duration of the connection. Since the state information is maintained for each established connection and the route of data packets is static, the data units are freed from the requirement to carry the full address of the required destination. The CO explicit relationship is established during the negotiation portion of the set-up phase and before the transfer phase. CO service provides for negotiation of the form of transmitted data and may maintain sequence and flow control. Error handling may also be supported. The overhead invested in setting up and maintaining a CO connection pays off when the data transfer phase is relatively long. The ITU-TS Recommendation X.25 for interfacing to a packet switching wide area network (WAN) is an example of a CO protocol.

In contrast, CL service has only one phase—namely, data transfer. The form of the data transferred must be pre-arranged between peer entities. Sequencing, flow control, and error handling are not supported by the CL service, but are instead the responsibility of the interacting peer entities. Sometimes referred to as a "datagram" service, CL service requires each data unit to be self-contained; there is no relationship between individual data unit transfers.

The goal of the OSI Reference Model is to limit the amount of a priori information exchanged between end systems regarding services used to communicate, which is best met by limiting the mixing of service modes. The following ISO/IEC standards for the four cases of connection orientation of the transport and network services are:

- ISO 8602 for CL transport and CL network
- ISO 8602 for CL transport and CO network
- ISO 8073 for CO transport and CO network
- ISO 8073 for CO transport and CL network.

The many resulting combinations of service are useful in different circumstances. CL service may be appropriate for military applications that require robust networks capable of continuing data transfer even as some nodes are taken out of service, especially for the lower layers (network and data link). [Ref. Purton 1987 and Stallings 1987a] give some additional examples of cases for which CL service is appropriate, even for the upper layers. Included are inward data collection from the sampling of data sources, broadcast messages, some distributed transactions, some real-time transmission applications, and cases in which one or more communicating peers are mobile. In general, CO service is beneficial when long-lived connections with extensive data transfer are anticipated. File Transfer, Access, and Management (FTAM) is an example of an application that would likely benefit from a CO connection.

The cases in which Layers 2 through 7 are all either CO or CL are more straightforward than cases with upper and lower layers of different orientation. If CL upper layers operate over CO lower layers, the full functionality of the lower layers is not employed; the application in this case does not enjoy the amenities of CO service.

The OSI standards supporting CO service were the first to be developed and are nearly complete. Until recently, standards supporting the lower layer CL service were more advanced than those supporting upper layer CL services. CL protocols for the Transport Layer (ISO 8602), Session Layer (ISO 9548), and Presentation Layer (ISO 9576) are complete.

Choice of connection orientation affects the structure of the Network Layer and to some degree the performance of services in the Network and Transport Layers. According to ISO 8648,

Internal Organization of the Network Layer, the Network Layer is divided into three sublayers. From top to bottom they are the Subnetwork Independent Convergence Protocol (SICP), the Subnetwork Dependent Convergence Protocol (SDCP), and the Subnetwork Access Protocol (SAP). This structure is preferred by many European countries. In a CL network, the Network Layer is divided into two sublayers: Internetwork Protocol (IP) and Subnetwork Specific Protocol (SSP), where the IP focuses on unreliable internetwork transfer of information while the SSP focuses on the reliable transfer of individual data units across the supporting networks. The CL approach is favored by the United States [compare the OSI profiles recommended by the United Kingdom and the United States given in Section 16.1.3, noting that ISO Class 4 Transport Protocol (TP4) provides services for CL networks]. In the CL model, end-to-end responsibilities are placed in the network sublayers, whereas in the CO approach the end-to-end requirements are placed in the Transport Layer. One drawback of using TP4 over a CO network is the size and complexity of the implementing code. For this and other reasons, many implementors of CO stacks do not support TP4. Section 6 of [Ref. NATO 1987] provides an analysis of the impact of the choice of CL or CO mode on the interconnection of heterogeneous military networks.

Architectural issues being developed in NATO, including those on connection orientation, are discussed in Section 18.9.3.

9.1.5 Quality of Service for OSI

Quality of service (QoS) is the collective name given to a set of parameters associated with data transmission between two peer service users, defining the quality of the service obtained during the exchange of data. Not all QoS parameters apply to all levels and some are dependent on whether the service provided is connection-mode or connectionless-mode operation. Some are subject to negotiation at the time of connection set-up and some are specified a priori. [Ref. Stallings 1993, p. 43] This is indicated, in part, by Table 14.

Table 14. Use of OSI Quality of Service Parameters

Quality of Service Parameter	Service Availability by OSI Layer						
	1	2	3	4	5	6	7
Residual error rate	C	C	C	N	N	P	P
Throughput	C	N	N	N	N	P	P
Transit delay	C	C	N	N	N	P	P
Protection	C	N	N	N	N	P	P
Priority		N	N	N	N	P	P
Resilience		C	C	N	C	P	P
Connection-establishment delay			C	N	C	P	P
Connection-release delay			C	N	C	P	P
Connection-establishment-failure probability			C	N	C	P	P
Transfer-failure probability			C	N	C	P	P
Connection-release-failure probability			C	N	C	P	P
Maximum acceptable cost			C				
Extended control					N	P	P
Optimized dialogue transfer					N	P	P

Key: C: Configured or selected prior to connection establishment.
N: Negotiated on a per-connection basis.
P: Parameter passed down to next lower layer.
Source: [Stallings 1993, p. 44].

9.2 Government/Military Requirements for OSI

NATO and many national agencies have hundreds of disparate information systems that are not interconnected and that include products from various vendors. The resulting heterogeneous environment may exhibit a high degree of incompatibility in terms of hardware, software, data, and communications. This incompatibility often leads to problems such as inefficiency, poor performance, high expense, as well as inhibiting interoperability. The *NATO OSI Profile (NOSIP) Strategy* [Ref. NATO 1993] and many national government OSI profiles (GOSIPs) have been developed to address these problems and are based on the standards shown in Figure 6 (above). These profiles (see Section 16.1.3) define and describe a common set of data communications protocols that enable systems developed by different vendors to interoperate and enable the users of different applications on these systems to exchange information.

9.2.1 Government Requirements for OSI

GOSIP is to be used by national agencies including defence communities when acquiring computer network products and services and communications systems or services that provide equivalent functionality to the protocols defined in GOSIP documents. In some cases (e.g., the United States), agencies will be permitted to buy network products in addition to those specified in GOSIP and its successor documents. Such products may include other non-proprietary protocols, proprietary protocols, and features and options of OSI protocols that are not included in GOSIP.

9.2.2 Military Requirements for OSI

During the past 8 years, NATO and the Nations have been assessing a number of deficiencies in the emerging OSI standards that need to be addressed for military needs. The eight deficiencies being addressed in TSGCE SG9 are (see Chapter 17 for definitions):

- Multimode, mobile host systems
- Multi-endpoint connection
- Internetworking
- Network/system management functions
- Security
- Robustness and quality of service
- Precedence and preemption
- Real-time and tactical communications.

With respect to the eighth military feature, *Real-time and Tactical Communication*, MITRE developed a proof-of-concept prototype system to test the applicability of GOSIP protocols in the tactical environment and concluded that the full OSI protocol stack could be used for tactical messages if the use of OSI Congestion Avoidance is required and the number of Message Transfer Agents (MTAs) that must be traversed is minimized. In addition, the architectures of the implementations must focus on efficient queue handling and connection handling. [Ref. Messing 1990]

Other efforts underway to evaluate potential OSI performance for tactical systems include a MITRE traffic study [Ref. Galitzer 1991] using loads of the US Maneuver Control System (MCS) traffic found in the MCS Segment Specification. Experiments were conducted that evaluated traffic between command posts and internal command post traffic between maneuver control and other battlefield functional areas (e.g., fire support). All of the experiment's messages were sent with normal priority and, at 600-bps delivery rates, all messages arrived in 15 minutes. Separate work

done by McArthur and Bryant [Ref. McArthur 1991] found that overhead generated by X.400 could seriously affect real-time and near-real-time tactical applications on low-bandwidth networks. For an example message with seven recipients, 3,532 octets (28,256 bits) of overhead were required. The authors note that overhead may be reduced by more efficient encoding or more selective use of X.400 parameters and concluded that it appeared that X.400 is not well suited for tactical applications that require real-time or near-real-time responses.

ISO SC21/WG1 is still refining the OSI Reference Model regarding the specification of the boundaries of Layers 1 and 2. Some of the protocols needed for the communications services may be determined to lie outside the Reference Model. These might include forward error correction coding[36] (several ISO standards provide for error detection) and other mechanisms such as interleaving of bits from a sequence of octets to reduce the impact of the environment on certain transmission media. Protocols for handling requirements of cryptographic devices (e.g., synchronization) and media access may also lie outside the Reference Model. Standardization of these features should, wherever possible, be accomplished with media-independent standards.

9.3 Physical Layer Standards

The physical layer covers the physical interface between devices and the rules by which bits are passed from one to another. The physical layer has four important characteristics (taken from [Stallings 1993, p. 37]):[37]

- *Mechanical*, relating to the physical properties of the interface to a transmission medium. Typically, the specification is of a pluggable connector that joins one or more signal conductors, called circuits.
- *Electrical*, relating to the representation of bits (e.g., in terms of voltage levels) and the data-transmission rate of bits.
- *Functional*, specifying the functions performed by individual circuits of the physical interface between a system and the transmission medium.
- *Procedural*, specifying the sequence of events by which bit streams are exchanged across the physical medium.

The physical layer differs from other OSI layers in that it cannot rely on a lower layer to transmit its protocol data units (PDUs); rather, it must make use of a transmission medium whose characteristics are not part of the OSI model. Because local area network (LAN) standards explicitly specify the physical media permitted for operation, the LAN standards are included in Part II (Physical Layer Standards) of Appendix D.

9.3.1 Communication Medium

Most digital data processing devices possess limited data transmission capability. Typically, they generate a simple form of digital signal known as NRZ (nonreturn to zero), in which a binary "1" is represented by a voltage pulse of constant amplitude, and binary "0" is represented by a voltage pulse of another amplitude. Such signals can be transmitted only over certain types of transmission media and over very limited distances. [Ref. Stallings 1993, pp. 48-49]

---

36 Whether forward error correction (FEC) is outside of the OSI Reference Model is still a contentious issue in ISO and NATO. Valid arguments exist for FEC at either Layer 1 or Layer 2.

37 The Physical Layer standards identified in Appendix D (Part II) are arranged in these four groups.

The types of media used as transmission medium are: twisted-pair cable, coaxial cable, fiber-optics, and microwave radio.

9.3.2 Twisted-Pair Cable

Twisted-pair cable is typically used for connecting point-to-point devices. The phone-wire approach to data cabling is often referred to as unshielded twisted-pair wire. Usually consisting of four pairs of 24-gauge, color-coded wires, it is the basis of new cabling provided to offices in today's voice-and-data wiring systems. In terms of quality, twisted-pair wiring used for telephones may not be equally capable as compared to the wiring used for data communications. Typical data rates vary from 56 kbps (thousands of bits per second) to 1 Mbps (millions of bits per second), though new technology is pushing the upper limit for twisted-pair cable to 10 Mbps. [Ref. Cerny 1991, p. 167]

9.3.3 Coaxial Cable

Coaxial cable comes in a wide variety of types covering a broad range of applications. Coaxial cable can be well shielded or poorly shielded; it can be thin and flexible or thick and rigid. The usable bandwidth for coaxial cable can be as high as 350 Mbps. This potentially high bandwidth can be utilized in one of the two ways [Ref. van der Jagt 1991, p. 159]:

- *Baseband mode*, in which all the available bandwidth is used to derive a single high bit rate (10 Mbps or higher) on the transmission medium.
- *Broadband mode*, in which the available bandwidth is divided to derive a number of lower bandwidth subchannels (and hence transmission paths) on a single cable. The amount of bandwidth required for each channel is determined by the desired data (bit) rate and the type of modulation method utilized, typically between 0.25 and 1.0 bits per Hz. Specifically, a 9.6-kbps channel may require on the order of 20 kHz of bandwidth and a 10-Mbps channel on the order of 18 MHz.

9.3.4 Fiber Optic Cable

Optical fibers are usually classified by the type of refractive index profile of their many layers of glass. Commonly used profile types are single-mode and multimode. In most types of fiber the outside cladding diameter is approximately 125 microns. The core diameter for single mode fiber is typically 8 microns, whereas multimode cores range from 50 to 100 microns in diameter. Lasers are used for long-distance communication and light-emitting diodes for cost sensitive applications that are limited in speed (250 Mbps) and distance (1 kilometer). [Ref. Cerny 1991, p. 167]

9.3.5 Interface Standards to Communications Media

A variety of standards that enable equipment to interface to communication media have been developed. Interoperability parameters for two of these (RS-449 and RS-423A) are defined in detail in Appendix A.

Connector standards have been available for more than 30 years. Many were developed and extended by the Electronic Industries Association (EIA). The following are the most common connector standards [Ref. Stallings 1991, pp. 134-142]:

- *RS-232C*,[38] a 25-pin connector with a specific arrangement of leads. It utilizes a signalling convention based on common ground, where a voltage more negative than

[38] RS232C is the third edition of RS-232, developed by EIA in 1969. The fourth edition, RS-232D (1987) differs in that it specifies only a cable connector and has three additional circuits for test operations.

-3V is interpreted as binary 1 and a voltage more positive than +3V is interpreted as binary 0. The interface is rated at a signal rate of less than 20 kbps and a distance of less than 15 meters (m).

- *RS-422-A* specifies balanced transmission and achieves a rate performance of 100 kbps at 1,200 m to 10 Mbps at 12 m.
- *RS-423-A* specifies unbalanced transmission and achieves a rate performance of 3 kbps at 1,000 m to 300 kbps at 10 m.
- *RS-449/* (37-pin connector) defines the mechanical, functional, and procedural aspects of the new interface and refers to RS-422-A and RS-423-A for defining electrical characteristics. Functionally, RS-449 retains all of the interchange circuits of RS-232-C, with the exception of protective grounds, and adds 10 new circuits. RS-449 has not received the popular adoption accorded to RS-232, partly due to the fact that its 37-pin interface requires more of a product's surface area than the 25-pin RS-232.
- EIA-530 was introduced in 1987 using the same 25-pin connector as for RS-232. EIA-530 is intended to operate at rates from 20 kbps to 2 Mbps. Unlike RS-232 and like RS-449, EIA-520 refers to RS-422-A and RS-423-A for defining electrical characteristics.

9.4 Data Link Layer Standards

9.4.1 Data Link Requirements

In the OSI model, the Data Link Layer provides the functional and procedural means to establish, maintain, and release data-link connections on behalf of network entities. The Data Link Layer attempts to make the Physical Layer reliable by providing error detection and control.[39] Data link control protocols are designed to deal with a variety of physical link characteristics and modes of operation including [Stallings 1993, p.37; Stallings 1987, pp. 70-83]:

- Point-to-point and multi-point link
- Long and short distance connections
- Half-duplex (two-way alternate) and full-duplex (two-way simultaneous) operation
- Primary-secondary (e.g., host-terminal) and peer (e.g., computer-to-computer) interactions.

In addition, data link layer protocols are intended to satisfy the objectives of code independence, adaptability, high efficiency, and high reliability.

There are two modes of data link service: character-oriented service (basic mode) and bit-oriented service. Standards for basic modes include ISO 1155, ISO 1177, ISO 1745, ISO 2111, ISO 2628, and ISO 2629 (see Section III.B of Appendix D). Bit-oriented services are provided by high-level data link control (HDLC) and integrated services digital network (ISDN); these are the most commonly used and are described in detail below.

Data link requirements can be met by bit-oriented synchronous data link protocols. A number of very similar bit-oriented protocols have achieved widespread use [Ref. Stallings 1991, p. 171]:

- HDLC, developed by ISO and widely used for point-to-point and multidrop configurations

[39] See Section 9.2.2 on military requirements for a comment on error correction services.

- Advanced data communication control procedures (ADCCP) developed by ANSI (ANSI X3.66) and adopted in the United States by NIST for use on federal procurements with very minor modifications[40]
- Logical Link Control (LLC), defined for LANs
- Link Access Procedure, Balanced (LAPB), used by ITU-TS as part of its X.25 packet-switched network standard
- Link Access Procedure, D-Channel (LAPD), used in ITU-TS's ISDN
- Synchronous Data Link Control (SDLC), developed and used by IBM, is not a standard but is in widespread use.

Small differences exist between HDLC and ADCCP. LAPB is a subset of HDLC. SDLC is also a subset of HDLC, but includes several additional features. A comparison of interoperability parameters for three military protocols derived from HDLC and ADCCP with the ISO standards is provided in Section 5 of Appendix C.

9.4.2 HDLC

The following are the key HDLC standards (see Section III.C of Appendix D):

- ISO 3309, *HDLC - Frame Structure*, Edition 4 (1991)
- ISO 4335, *HDLC - Elements of Procedures*, Edition 4 (1991)
- ISO 7776, *HDLC - Description of the X.25 LAPB-Compatible DTE Data Link Procedures*
- ISO 7809, *HDLC - Consolidation of Classes of Procedures*, Edition 2 (1991)
- ISO 8471, *HDLC Balanced Classes of Procedures - Data Link Layer Address Resolution/Negotiation in Switched Environments*
- ISO 8885, *HDLC - General Purpose XID Frame Information Field Content and Format*, Edition 2 (1991).

HDLC uses synchronous transmission. All transmissions are in frames, and a single frame format suffices for all types of data and control exchanges. The frame has the following fields [Ref. Stallings 1993, p. 58; Stallings 1991, p. 173]:

- Flag (8 bits)—appears at the beginning and end of each frame and is used for synchronization
- Address (one or more octets)—indicates the secondary station for a transmission; it is needed in the case of a multidrop line, where a primary may send data to one of a number of secondaries and one of a number of secondaries may send data to the primary
- Control (8 or 16 bits)—identifies the purpose and functions of the frame (see below)
- Information (variable octets)—contains the user data to be transmitted
- Frame Check Sequence (16 or 32 bits)—used in the mode of a cyclic redundancy check for error detection.

HDLC defines three types of frames, each with a different control-field format. Information frames (I-frames) carry the user data to be transmitted for the station. Additionally, information frames contain control information for flow control and error control. The supervisory frames (S-frames) provide another means of exercising flow control and error control. Unnumbered frames (U-frames) provide supplemental link-control functions. Use of these frame

---

40 Two examples of military protocols derived from ADCCP are given in Appendix C (Sections 3 and 4).

types and some of the 14 HDLC options are illustrated in Sections 3-5 of Appendix C. [Ref. Stallings 1993, p. 59]

9.4.3 Multilink Procedure

HDLC and most other link control protocols are designed to operate over a single physical circuit between two systems. In some cases, multiple parallel physical circuits exist between a single pair of systems. ISO has defined a multilink procedure (MLP) to operate over multiple lines to achieve greater throughput and reliability (ISO 7478, *Multilink Procedures*). Over each line, a single link procedure, such as HDLC, is used. The MLP operates above the single link procedure, and may be thought of as an upper sublayer of the data link layer. [Ref. Stallings 1993, p. 64]

When a Layer 3 protocol data unit (PDU) is presented to the MLP for transmission, any available link may be chosen. Indeed, the MLP may assign successive PDUs to different links to satisfy throughput or availability constraints. [Ref. Stallings 1987, p. 92]

9.4.4 Logical Link Control (LLC)

LLC is the data link standard defined for local area networks (ISO 8802-2, *Local Area Networks*, Part 2: *Logical Link Control*). A revision of the 1989 edition of this standard is in progress and has reached DIS status.

LLC makes use of only the asynchronous *balanced* mode of operation of HDLC. The key difference between LLC and the traditional standards, such as HDLC, is that LLC is designed to operate over a peer multi-point link (termed "multiplexing"). In this case, there are multiple devices attached to a transmission medium, all of which are capable of initiating transmission; there is no unique primary on the link. To account for this, each transmitted data unit includes both the sending and receiving address, rather than just the address of a secondary. [Ref. Stallings 1987, p. 97]

The LLC standard specifies three types of services that may be offered to the network layer [Ref. Stallings 1993, pp. 321-324]:

- Type-1—unacknowledged connectionless service, which has the same characteristics as any OSI connectionless-mode service, provides no flow control or error control, and does not guarantee the delivery of data in the order in which they were sent
- Type-2—connection-oriented service, which is similar to the connection-mode network service
- Type-3—acknowledged connectionless service, which provides a mechanism by which a user can send a unit of data and receive an acknowledgment that the data were delivered, without the necessity of setting up a connection.

A system can support more than one of these types in the following combinations: Type 1 alone, Types 1 and 2, Types 1 and 3, and all three types. (Type 1 is mandatory.)

9.4.5 LAPB

LAPB is designed for use on X.25, which, like LLC, is a subset of the asynchronous *balanced* mode of HDLC. LAPB is restricted to Options 2, 8, and 10 of the 14 options permitted by HDLC. LAPB is the most commonly specified form of HDLC for wide area networks (WANs). It is used for point-to-point link between a user system (termed data terminal equipment or DTE) and a packet switched network node (an example of a data circuit-terminating equipment or DCE). When multiple links exist between DTE and DCE, each link is governed by LAPB. It is

also used in LANs, where packets flow in only one direction at a time. [Ref. Stallings 1987, p. 113; Stallings 1993, p. 63]

9.4.6 LAPD

LAPD is a data link standard (ITU-TS I.441) developed as part of the ISDN standardization effort. It specifies a link access protocol to be used over a logical channel, known as the D-channel, that is part of a time-multiplexed link between a network subscriber and the ISDN central office. LAPD is a variant of HDLC, based on LAPB. [Ref. Stallings 1987, p. 97]

LAPD provides two forms of service to users: unacknowledged information transfer service and acknowledged information transfer service. The unacknowledged information transfer service simply provides for the transfer of frames containing user data with no acknowledgment, no guarantee of data delivery, no notice if the delivery attempt fails, no flow control, and no error control. This service supports both point-to-point (deliver to one user) and broadcast (deliver to a number of users), allows for fast data transfer, and is useful for management procedures such as alarm messages and messages that need to be broadcast to multiple users. The acknowledged information transfer service is the more common one and is similar to the service offered by LAPB and HDLC. With acknowledged information transfer service, a logical connection is established between two LAPD users prior to the exchange of data. [Ref. Stallings 1993, p. 228]

LAPD has to deal with two levels of multiplexing. First, at a subscriber site, there may be multiple user devices sharing the same physical interface. Second, within each user device, there may be multiple types of traffic, especially packet-switched data and control signalling. To accommodate these levels of multiplexing, LAPD employs a two-part address, consisting of a terminal endpoint identifier (TEI) and a service access point identifier (SAPI). Typically, each user device is given a unique TEI. It is also possible for a single device to be assigned more than one TEI. This might be the case for a terminal concentrator. The SAPI identifies traffic type. [Ref. Stallings 1987, p. 97]

9.5 LAN Technologies

There are many ways to view LAN technologies and to categorize LANs. One of the more common ways is to group them by transmission and switching technologies. The categories are [Ref. Slone 1991, pp. 80-82]:

- Baseband LANs were the first to be used on a large scale basis. Their distinctive feature is their use of a single transmission medium and a single transmission channel. Because baseband LANs were the first to be widely used, support equipment such as bridges, gateways, servers, and test equipments are readily available.
- Broadband LANs employ many of the technologies used by the cable television industry. For example, broadband LANs and cable television generally use the same coaxial cable, amplifiers, splitters, couplers, and taps. To adapt this technology for data transmission, radio frequency modems are used to convert the digital data signals into analog signals. These signals sit on one of the many cable channels in the same way that different television channels are carried on commercial cable systems.
- Switched-Based LANs are of different types, including private branch exchanges (PBXs) and telephone companies' central offices. These LANs are capable of providing both circuit and packet switching on a single network. Circuit switching is more suitable for calls that transmit large amounts of data for a relatively long period of time, whereas low-volume, interactive traffic is more efficiently served by packet switching. Neither baseband or broadband LANs are well suited for circuit switching.

- Hybrid LANs. Several other types of LANs are available, but they are primarily hybrids or adaptations of the types discussed. Another hybrid is a combined voice and data version of Fiber Distributed Data Interface (FDDI), a high-speed fiber network standard being developed by ANSI (see Section 9.5.7). This network is technologically a baseband system because all devices share a single digital channel on a single medium.

9.5.1 LAN Standards

The IEEE 802 working groups were chartered to create standards by which devices could communicate over LANs. The working groups have created a flexible framework for LANs spanning the lower two OSI levels, including network management and internetworking of these layers. Table 15 depicts the model used for LAN standards.

Table 15. Model for LAN Standards

OSI Layer	LAN Model Layer
Data Link Layer	Logical Link Control (LLC)
	Media Access Control (MAC)
Physical Layer	Physical Layer Protocol
	Physical Layer—Media Dependent Specifications

Source: [Stallings 1993, p. 319].

The LAN functions associated with the OSI Data Link Layer include [Ref. Stallings 1993, p. 320]:

- Providing one or more service-access points (SAPs)
- On transmission, assembling data into a frame with address and cyclic redundancy check (CRC) fields
- On reception, disassembling the frame and performing address recognition and CRC validation
- Governing access to the LAN transmission medium.

The first function and related functions are grouped into the logical link control (LLC) sublayer. The last three functions are treated as a separate layer, called medium-access control (MAC) sublayer. LAN standards include the MAC-to-physical layer interface and the MAC-to-LLC interface.

The physical layer includes such functions as encoding/decoding of signals, preamble generation/removal (for synchronization), and bit transmission/reception. In addition, the physical layer of the LAN model includes a specification of the transmission medium. Generally, this is considered below the lowest layer of the OSI model. However, the choice of transmission medium is critical in LAN design, and so a specification of the medium is included. [Ref. Stallings 1993, p. 319]

Table 16 identifies the current LAN standards. It shows that second editions of ISO 8802-1 and ISO 8802-2 are in progress and have reached DIS stage. These will update the original standards adopted in 1987 and revised in 1989. Edition 3 of ISO/IEC 8802-3 was approved and distributed in 1992. At that time, the title of ISO 8802 was changed from *Local Area Networks* to *Local Area Networks and Metropolitan Area Networks (MANs)*.

Table 16. LAN Standards

IEC 847	Characteristics of LANs, 1988
IEC/TR 907	Local Area Networks CSMA/CD 10 Mbps Baseband Planning and Installation Guide
ISO 8802-1	LANs, Part 1: General Introduction, 1989
DIS 8802-1.2	LANs and MANs, Part 1: General Introduction with System Load Protocol
ISO 8802-2	LANs, Part 2: Logical Link Control, 1989
DIS 8802-2.2	LANs and MANs, Part 2: Logical Link Control, Edition 2 (draft)
DAM 1	Flow Control Techniques for Bridged LANs
DAM 2	Type 3 Operation - Acknowledge Connectionless Service
DAM 3	PICS Proforma
DAM 4	Editorial Changes and Technical Corrections
PDAM 5	Bridged LAN Source Routing Operations by End Systems
ISO/IEC 8802-3	LANs and MANs, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Access Method and Physical Layer Specifications, Edition 3, 1993
ISO/IEC 8802-4	LANs, Part 4: Token-Passing Bus Access Method and Physical Layer Specifications, 1990
ISO/IEC 8802-5	LANs and MANs, Part 5: Token Ring Access Method and Physical Layer Specifications, 1992
DIS 8802-6	LANs, Part 6: Distributed Queue Dual Bus (DQDB) Media Access Control (MAC)
ISO/IEC 8802-7	LANs, Part 7: Slotted Ring Access Method and Physical Layer Specification, 1991
DIS 8802-9	LANs, Part 9: Integrated Voice and Data (IVD) LAN
CD 8802-51	LANs, Part 51: MAC Sublayer Conformance Test Purposes
ISO/IEC 8881	Use of the X.25 Packet Level Protocol (PLP) in Local Area Networks
ISO 9314-1	Fiber Distributed Data Interface (FDDI), Part 1: Physical Layer Protocol (PHY)
TR 9578	Communication Interface Connectors Used in LANs
DIS 10038	MAC Sublayer Interconnection (MAC Bridging)
PDAM 1	Specification of Management Information for CMIP
DAM 2	Source Routing Supplement
ISO/IEC 10039	MAC Service Definition
ISO/IEC TR 10178	Structure and Coding of Link Service Access Point Addresses in LANs
ISO/IEC TR 10738	Recommended Practice for Use of Unshielded Twisted Pair Cable (UTP) for Token Ring Data Transmission at 4 Mbps

9.5.2 CSMA/CD LANs

In carrier sense multiple access with collision detection (CSMA/CD; ISO/IEC 8802-3), a station wishing to transmit first listens to the medium to determine whether another transmission is in progress (carrier sense). If the medium is idle, the station may transmit. It could happen that two or more stations attempt to transmit at about the same time; if this occurs, there will be a collision—the data from both transmissions will be garbled and not received successfully. CSMA/CD specifies what a station should do if the medium is found to be busy and what to do if a collision occurs. [Ref. Stallings 1993, p. 327]

The following are the medium-dependent physical layer standards incorporated into the CSMA/CD (sometimes called Ethernet) standard [Ref. Stallings 1993, pp. 330-356]:

- 10BASE5[41]—10-Mbps baseband system using 50-ohm coaxial cable (10-mm diameter) with a maximum segment length of 500 m; its length can be extended to 2,500 m by use of repeaters
- 10BASE2—10-Mbps baseband system using a smaller (5-mm diameter) 50-ohm coaxial cable with a maximum segment length of 185 m; its length can be extended to

[41] The structured name specifies baseband (BASE) or broadband (BROAD) transmission; bit rate in Mbps (e.g., 10 in 10BASE5 denotes 10 Mbps), and approximate maximum segment length in hundreds of meters (e.g., 5 in 10BASE5 denotes 500 m).

925 m by use of repeaters (10BASE2 is a lower cost option than 10BASE5 applicable for personal computers)

- 1BASE5—1-Mbps baseband system using unshielded twisted-pair cable (ordinary telephone wire, 0.4-0.6-mm diameter) with a maximum segment length of 500 m; its length can be extended to 2,500 m by use of repeaters (1BASE5 is an even lower cost option than 10BASE5 that uses standard telephone wiring typical of many building installations)
- 10BASET—10-Mbps baseband system using twisted-pair cable with a maximum segment length of 100 m; its length can be extended to 500 m by use of repeaters (this variant of 1BASE5 trades increased bandwidth for decreased maximum segment length)
- 10BROAD36—10-Mbps broadband system using 75-ohm coaxial cable (standard for cable television; 0.4-1.0-mm diameter) with a maximum segment length of 3,600 m (two 1,800-m segments from a head-end).
- 100BASET—100-Mbps baseband system using fiber or twisted-pair cable (this is still under development).
- 100VG-AnyLAN—expected to provide a 100 Mbps migration path from 10-Mbps CSMA/CD and 16-Mbps token ring networks; combines 100-Mbps transmission with a MAC layer that operates over Category 3, 4 or 5 unshielded twisted-pair, shielded twisted-pair, and optical fiber.

9.5.3 Token Bus LANs

For a token bus LAN (ISO/IEC 8802-4), the stations on the bus or tree form a logical ring, in which the stations are assigned logical positions in an ordered sequence and for which the last member of the sequence is followed by the first. Each station knows the identity of the station preceding and following it. The physical ordering of the stations on the bus is irrelevant to and independent of the logical ordering. A control frame, known as the token, regulates the right of access. The token contains a destination address. The station possessing the token is granted control of the medium for a specified time. The station may transmit one or more frames and may poll stations and receive responses. When the station is finished or time has expired, it passes the token to the next station in logical sequence. This station now has permission to transmit. Hence, normal operation consists of alternating data-transfer and token-transfer phases. In addition, non-token-using stations are allowed on the bus; they can only respond to polls or request for acknowledgment. [Ref. Stallings 1993, p. 339]

The following are the medium-dependent physical layer standards incorporated into this standard [Ref. Stallings 1993, pp. 347-349]:

- Phase-continuous carrier band—1-Mbps phase-continuous carrier band, using a form of frequency-shift keying (FSK), in which the transition between signalling frequencies is accomplished by a continuous change of frequency, as opposed to the discontinuous replacement of one frequency by another, resulting in a tighter bandwidth and improved transmission and reception efficiency. Digital data are transmitted using Manchester encoding and then passed through a modem at 6.25 MHz (high) and 3.75 MHz (low).
- Phase-coherent carrier band—the phase-coherent FSK carrier band, using a data rate of 5 and 10 Mbps (phase coherent means that the two signalling frequencies are integrally related to the data rate, ensuring that the zero crossing points are in phase at the beginning and end of each bit time).

- Broadband—the broadband specification allowing for data rates of 1, 5, and 10 Mbps, with bandwidths of 1.5, 6, and 12 MHz, respectively. The standard recommends the use of a single-cable system with a head-end frequency translator. Dual cable is also permitted.
- Optical fiber—allowing three data rates: 5, 10, and 20 Mbps. In keeping with standard practice for optical fiber systems, the bandwidth and carrier are specified in terms of wavelength (nm or nanometers). For all three data rates, the bandwidth is 270 nm, and the center wavelength is between 800 and 910 nm.

9.5.4 Token Ring LANs

Intended for use in commercial, military, and light industrial environment, a token ring is composed of a number of stations serially connected by a medium. As for token bus, the media access control protocol (ISO/IEC 8802-5) is based on use of a frame called a token. The token circulates on the ring when all stations are idle. A station wishing to transmit must wait until it detects a token passing by. It then seizes the token (by changing one bit in the token and changing it to a start-of-frame sequence for a data frame) and appends the rest of a data frame. When a station seizes the token and begins to transmit a data frame, there is no token on the ring, so other stations wishing to transmit must wait. The frame on the ring will make a round trip and be absorbed by the transmitting station, which will then insert a new token on the ring. Once the new token has been inserted on the ring, the next station downstream with data to send will be able to seize the token and transmit. [Ref. Stallings 1993, p. 350-351]

The standard specifies the use of shielded twisted-pair wire with data rates of 4 and 16 Mbps. Differential Manchester encoding is used. The unshielded twisted-pair version operates at 4 Mbps. [Ref. Stallings 1993, p. 356] A new standard for this is ISO/IEC TR 10738, *Token Ring Access Method and Physical Layer Specifications - Recommended Practice for Use of Unshielded Twisted Pair Cable (UTP) for Token Ring Data Transmission at 4 Mbit/s*, 1993.

9.5.5 Metropolitan Area Networks (MANs)

The MAN standard (DIS 8802-6; ANSI/IEEE 802.6) was designed to occupy a middle ground between the LAN and wide area networks (WANs). The standard is referred to as the distributed-queue dual-bus (DQDB) subnetwork standard, since medium-access control is based on the maintenance of distributed queues. [Ref. Stallings 1993, pp. 389-390, 433] A MAN has two separate unidirectional buses, both of which carry data at the same time. Reconfiguration is possible when a link breaks (and with looped topology, full connectivity is maintained).

The medium access control protocol is based on time division multiple access. It uses reservations, where the time is divided into continuous, discrete time segments (frames) of 125 μs. Each frame is subdivided into a number of 53-octet cells, depending on the speed of the channel. Because of compatibility of cell size, MANs can be readily integrated with asynchronous-transfer-mode (ATM)-based broadband ISDN and other networks based on ATM (see Section 9.6.3).

The medium-access-control technique is based on the maintenance of distributed queues, in which each node maintains queues of outstanding requests that determine access to the MAN medium. This DQDB scheme supports both packet mode and isochronous[42] mode data transfer.

[42] ISO 2382 defines isochronous transmission as a data transmission process in which there is always an integral number of unit intervals between any two significant events.

The transmission systems currently specified are [Ref. Stallings 1993, p. 407-408]:

- ANSI SONET STS-3c (ITU-TS Synchronous Digital Hierarchy)—transmits data at 155.52 Mbps and above over a single-mode fiber (see Section 9.6.1)
- ITU-TS G.703—transmits data at 34.368 Mbps and 139.264 Mbps over a metallic medium
- ANSI DS3—transmits data at 44.736 Mbps over 75-ohm coaxial or fiber media and provides a frame size of 595 octets and a frame duration of 106.4 µs; it is a commonly used transmission system for North America.

9.5.6 Wireless LANs

IEEE 802.11 is working on a wireless LAN standard, with a draft expected early in 1994.

9.5.7 FDDI LANs

9.5.7.1 FDDI LAN Standards

The Fiber Distributed Data Interface (FDDI) standards are the following:

- ISO 9314-1, *FDDI, Part 1: Physical Layer Protocol* [ANSI X3.148-1988]
- ISO 9314-2, *FDDI, Part 2: Media Access Control (MAC)* [ANSI X3.139-1986]
- ISO/IEC 9314-3, *FDDI, Part 3: Physical Layer Medium Dependent (PMD)* [ANSI X3.166-1990]
- ISO/IEC 9314-4, *FDDI, Part 4: Single-Mode Fiber/Physical Layer Medium Dependent* [ANSI X3.184-1993]
- DIS 9314-5, *FDDI, Part 5: Hybrid Ring Control (FDDI-II)* [ANSI X3.186-199X]
- CD 9314-6, *FDDI, Part 6: Station Management (SMT) Standard* [ANSI X3.229-199x].

The FDDI is a set of standards developed by ANSI X3T9.5. Basic FDDI supports a packet-mode data transfer service. The timed token access method, used to share the medium among stations in this 100-Mbps LAN, differs from the traditional token ring method (ISO/IEC 8802-5) in that the time for the token to walk around the ring is accurately measured by each station and used to determine the usability of the token. Two differences from the token ring LAN are as follows [Ref. Stallings 1993, p. 367]:

- In FDDI, a station waiting for a token seizes the token by aborting (failing to repeat) the token transmission as soon as the token frame is recognized (rather than flipping a bit in the token to the start of a data frame, which is less efficient). After the captured token is completely received, the station begins transmitting one or more data frames.
- In FDDI, the station that has been transmitting data frames releases a new token as soon as it completes data-frame transmission (a technique known as early frame release), which is more efficient than waiting for its frame to return as in normal token ring operation.

The FDDI standard encompasses both the MAC and physical layers. FDDI defines two types of traffic: synchronous and asynchronous. Each station is allocated a portion of the total capacity (this portion may be zero); the frames that it transmits during this time are referred to as synchronous frames. Any capacity that is not allocated or that is allocated but not used is available for the transmission of additional frames, referred to as asynchronous frames. [Ref. Stallings 1993, pp. 364, 369]

The FDDI standard specifies an optical-fiber ring with a data rate of 100 Mbps, using NRZI-4B/5B encoding scheme. The wavelength specified for data transmission is 1,300 nm. The

dimensions of the fiber cable are specified in terms of the diameter of the core fiber and the outer diameter of the cladding layer that surrounds the core. The combination specified in the standard is 62.5/125 μm (micro-meter). The standard lists as alternatives 50/125, 82/125, and 100/140 μm. [Ref. Stallings 1993, p. 380]

The SMT standard (CD 9314-6) provides the control necessary at the station (node) level to manage the processes underway in the various FDDI layers such that a station (node) may work cooperatively as a part of an FDDI network. It will provide such services as connection management, station insertion and removal, station initialization, configuration management, fault isolation and recovery, communications protocol for external authority, scheduling policies, and collection of statistics. [Ref. X3 1992d]

9.5.7.2 FDDI-II LAN Standards

FDDI-II is an upward-compatible extension to FDDI that adds the ability to support circuit-switched (isochronous) traffic, in addition to the packet-mode traffic supported by basic FDDI. With FDDI-II, it is possible to set up and maintain a constant-data-rate connection between two stations using a regularly repeating (125-μs-long) time slots in the frame. At 100 Mbps, each cycle permits 12,500 bits to be transmitted. This capability is divided into sixteen 96-octet channels, each with a capacity of 6.144 Mbps. These channels can be subdivided into subchannels to support compressed voice and data (1-4 bits per cycle, 8-32 Kbps), voice or ISDN B-channel (8 bits per cycle, 64 Kbps), ISDN H0 (48 bits per cycle, 384 Kbps), ISDN H11 channel (192 bits per cycle, 1,536 Kbps), and T1 carrier (193 bits per cycle, 1,544 Kbps). [Ref. Stallings 1993, p. 391-395]

9.5.7.3 FDDI Follow-On LAN Standards

Another high-speed version of FDDI, called FDDI follow-on LAN (FFOL) and designed for data rates of 622 Mbps to 1.2 Gbps, has been proposed by ANSI X3T9.5. The general requirements for FFOL include:

- The ability to provide a backbone for multiple FDDI networks
- The ability to provide efficient interconnections to wide area networks [e.g., Broadband-ISDN (BISDN)]
- The ability to support for a wide variety of "integrated" services such as data, graphics, video, and audio
- An initial data rate less than 1.25 Gbps
- A data rate matched to ITU-TS Synchronous Data Hierarchy (SDH), another fiber-based system that provides support for communication in the 100- to 622-Mbps range (ITU-TS G.707, G.708, and G.709) (see Section 9.6.1)
- The ability to use existing FDDI cable, where feasible.

The target date for completion of the basic FFOL standards is December 1995. The estimated life of the FFOL family of standards is 10 to 15 years. In May 1991, ASC X3 announced the approval of six new FFOL projects to be developed by ANSI X3T9.5, as follows:

- FFOL - Physical Medium Dependent (FFOL-PMD)
- FFOL - Physical Layer Protocol (FFOL-PHY)
- FFOL - Service Multiplexer (FFOL-SMUX)
- FFOL - Asynchronous Media Access Control (FFOL-AMAC)
- FFOL - Isochronous Media Access Control (FFOL-IMAC)
- FFOL - Station Management (FFOL-SMT).

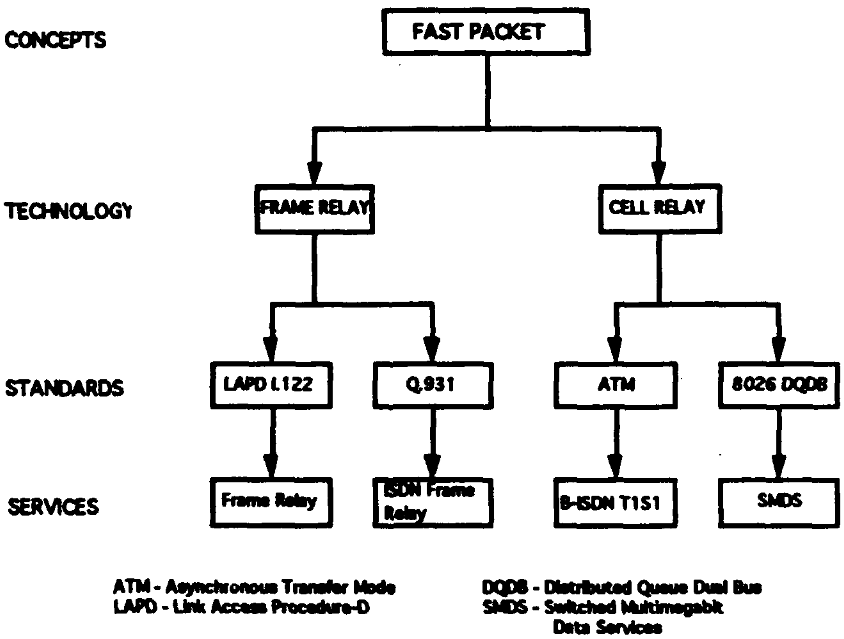
9.5.7.4 Low-Cost Fiber FDDI Standards Development

A new proposed standard for low-cost fiber (LCF) optic connections to FDDI is under consideration. This draft standard, *FDDI-LCF-PMD* defines a smaller lower-cost connector and optical specification for connections that are primarily intended for horizontal cabling from the wiring closet to the desktop. [Ref. X3 1992j]

9.6 Broadband Technology

Broadband technology is based on the concept of "fast packet" (see Figure 7), which appears as frame relay and cell relay. Frame relay is an extension of circuit switching, whereas cell relay is an extension of packet switching. Frame relay uses variable-length packets (the frames), reduces the overhead associated with circuit switching to take advantage of low-error-rate transmission means, and operates at rates of up to 2 Mbps (compared to 64 Kbps for circuit switching). Frame relay standards being developed by ITU-TS include I.122, *Framework for Providing Additional Packet Model Bearer Services,* for LAPD and Q.931 for ISDN frame relay. Another example of frame relay is the synchronous optical network (SONET), an ANSI standard whose counterpart in ITU-TS is known as synchronous digital hierarchy (SDN). [Ref. Stallings 1993, pp. 243, 277-278]

In cell relay, there are fixed-length frames of 53 octets, of which 48 are data and the others are overhead for error control. Cell relay is designed to work in the range of tens to hundreds of megabits per second. Examples of cell relay standards are ISO 8802-6 (MAN) and ATM for wide area networks.



Source: [Davidson 1991, p.78].

Figure 7. Broadband Technology

9.6.1 SONET

The Synchronous Optical Network (SONET) is an optical transmission interface standardized by ANSI. A comparable version, referred to as SDH (Synchronous Digital Hierarchy), has been published by ITU-TS in recommendations G.707, G.708, and G.709. Each is intended to provide a specification for taking advantage of the high-speed digital transmission capability of optical fiber. The SONET specification defines a hierarchy of standardized digital data rates, illustrated in Table 17. These rates are based on multiples of 3 times 810 octets transmitted once every 125 µs (27 of the 810 octets are overhead, for an efficiency of 96.7 percent). ANSI designations are specified in terms of the synchronous transport signal level (STS) and corresponding optical carrier level (OC), whereas ITU-TS designations are in terms of the synchronous transfer mode level (STM). Related ITU-TS recommendations and ANSI standards are listed in Table 18. [Ref. Stallings 1993, pp. 300-303]

Table 17. SONET Digital Data Rates

SONET Designation	ITU-TS Designation	Data Rate (Mbps)
STS-1/OC-1	-	51.84
STS-3/OC-3	STM-1	155.52
STS-9/OC-9	STM-3	466.56
STS-12/OC-12	STM-4	622.08
STS-18/OC-18	STM-6	933.12
STS-24/OC-24	STM-8	1244.16
STS-36/OC-36	STM-12	1866.24
STS-48/OC-48	STM-16	2488.32

Source: [Stallings 1993, p. 301].

Table 18. ITU-TS Recommendations and ANSI Standards on SONET

Standard/ Recommendation	Subject
ITU-TS G.707 to G.709	SDH Rates and Format
ITU-TS G.781 to G.784	Equipment Functions
ITU-TS G.957	Optical Interfaces
ITU-TS G.958	Line Systems
ITU-TS G.803	Network Architecture
ITU-TS G.831	Management Capabilities
ITU-TS G.774	Management Information Model
ANSI T1.105	SONET Rates and Format
ANSI T1.106	Optical Parameters (superseded by G.957 and TR 253)
ANSI T1.117	Optical Parameters-Short Reach
ANSI T1.118	OAM&P Communications

Source: [Davidson 1991, p.78].

SONET addresses the incompatibility of European and North American schemes for high-data-rate transmissions (in excess of the ANSI DS3 44.736-Mbps level) in optical systems by providing a standardized hierarchy of multiplexed digital transmission rates that accommodates both the ITU-TS and North American existing rates. SONET also addresses the need for economic access to small amounts of traffic within the bulk payload of an optical signal by introducing a new approach to time-division multiplexing. Further, SONET addresses the need for a major increase in network management capabilities within the synchronous time-division signal

to enable services such as virtual private networking, time-of-day bandwidth allocation, and support of the broadband ISDN ATM technique. [Ref. Stallings 1993, p. 300]

The basic SONET building block is the STS-1 frame, which consists of 810 bytes and is transmitted once every 125 μs, for an overall data rate of 51.84 Mbps. The first 27 octets of the frame are devoted to overhead, with 9 octets devoted to section-related overhead and 18 octets defining various fields. The remainder of the frame is payload. STM-1 (155.52) is the lowest ITU-TS level, as it is the lowest-rate signal that can accommodate the ITU-TS level-four signal of 139.264 Mbps. [Ref. Stallings 1993, pp. 300-303]

9.6.2 BISDN

Broadband ISDN (BISDN) provides a wide range of services through flexible user-network interfaces over a limited number of connection types. BISDN can include a switched or non-switched network connection. BISDN supports all the 64-kbps transmission services, both circuit-switching and packet switching, provided by ISDN and, in addition, provides for higher-data-rate transmission services.[43] The fast-packet-switching technique of BISDN readily supports the user-network interface protocol known as asynchronous transfer mode (ATM).

The BISDN can offer different forms of applications and communications capabilities. The communications and applications could support distribution oriented services and/or interactive services. These services include: conversational, messaging, retrieval services, and distribution services with and without individual presentation control. Conversational services are those services that provide bidirectional (although unidirectional could be included) dialogue communications. These services could include video surveillance, video-telephony, video teleconference, and high speed data communications.

Message services are the "typical" mail functions extended to films or moving pictures, high resolution images, and audio information. These services allow a user to create, edit, process, convert, store, and forward messages. This service allows end users to communicate with each other.

Retrieval services allow an end user to retrieve information from a "central" location or archive site. The information could be film, high resolution image, or audio information. The information is retrieved on demand. The archive site only delivers requested information.

Distribution services can exist with or without individual presentation control. Distribution services without individual presentation control include broadcast services for television. A television viewer can select a channel, but has no control over the presentation. The start and finish of the presentation is under the control of the distribution service. A distribution service with individual presentation control broadcasts in a cyclic manner. Upon user selection, the user receives the presentation from its beginning.

9.6.3 Asynchronous Transfer Mode (ATM)

Sometimes known as cell relay, ATM was developed for use with Broadband ISDN, which, as noted above, is based on optical fiber cable and is intended to support transfer of voice, data, and video at rates on the order of 150 Mbps (applications on the order of 600 Mbps are also being considered). ATM is, in effect, a packet-oriented protocol based upon a relatively short,

---

[43] Note that ISDN concepts include broadband—the terminology B-ISDN exists only to focus attention on the broadband aspects of ISDN, which can handle audio, video, and data communications. ISDN is discussed in connection with the Network Layer in Section 9.7.6. ISDN standards are listed in Section II.B of Appendix E.

fixed-length frame (called a cell), supporting a hierarchical structure of virtual channels and virtual paths (that contain one or more virtual channels), over multiple physical links. The ATM is a connection-oriented technique that can be used to support both connection-oriented and connectionless services. Signalling (such as call set up and clear) and user information are carried on separate virtual channels. ATM is designed to offer a flexible transfer capability common to all services.

The ATM standard is being developed by ITU-TS SGXVIII. Although ATM assumes an optical fiber physical medium, other media are being considered for ATM use including satellite transmission. The size (48 octets) of the payload for each ATM cell is a compromise between a larger size (64 octets) favored by the United States and Japan and a small size (16 octets) favored by representatives from Europe.

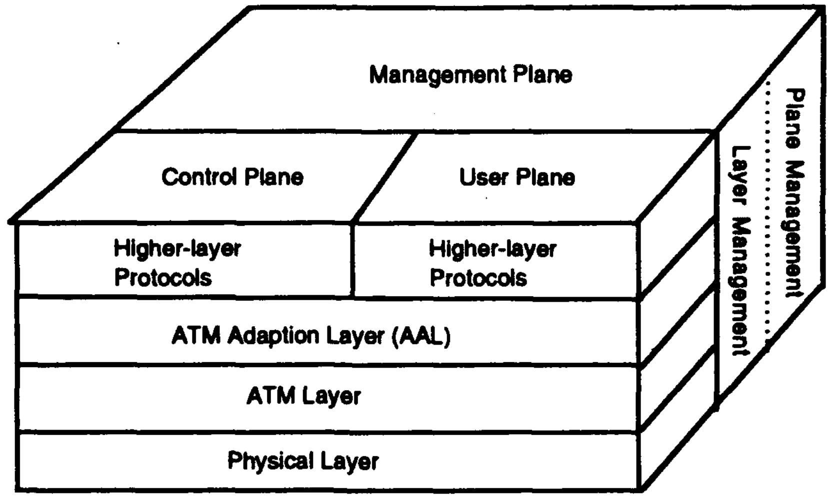
9.6.3.1 ATM Model

Figure 8 is an illustration of the protocol architecture for BISDN that shows the two layers for ATM. These layers are the ATM layer and the ATM adaptation layer (AAL). The ATM layer provides generic flow control, cell-header generation and extraction, cell virtual path identifier (VPI) and virtual channel identifier (VCI) translation, and cell multiplexing and demultiplexing. (Network management for ATM is simplified by dividing the transmission path into one or more virtual paths, each of which is subdivided into one or more virtual channels.) These functions are common to all services that provide packet-transfer capabilities, whereas the AAL is service dependent. The AAL maps higher-layer information into ATM cells and collects information from ATM cells for delivery to high layers. The functions provided by the AAL (for which there are corresponding sublayers) are convergence (CS) and segmentation and reassembly (SAR). The AAL supports information-transfer protocols not based on ATM, such as pulse code modulation (PCM) and LAPD (e.g., using SAR to map LAPD frames into ATM packets and recover the LAPD frames after transmission). [Ref. ITU-TS I.121:1990; Stallings 1993, p. 274, 279]

ITU-TS I.413:1990 specifies two approaches to the physical layer for 155.52-Mbps interface: one that is cell-based and one that is SDH (SONET)-based. For the cell-based physical layer, no framing is imposed—the interface structure consists of a continuous stream of 53-octet cells. The SDH-based physical layer uses the STM-1 (STS-3/OC-3) 810-octet frame (see Section 9.6.1).

The model specifies three planes orthogonal to the layers [Ref. Stallings 1993, p. 274-275]:

- User plane—provides for user information transfer, along with associated controls (e.g., flow control, error control)
- Control plane—performs call-control and connection-control functions
- Management plane—includes plane management, which performs management functions related to a system as a whole and provides coordination between all the planes; and layer management, which performs management functions related to resources and parameters residing in its protocol entities.



Source: [ITU-TS I.121:1990; Stallings 1993, p. 273].

Figure 8. ATM Protocol Reference Model

9.6.3.2 ATM Support of Military Features

In its analysis of ATM, MITRE has noted the following with regard to military features for ATM [Ref. MITRE 1990]:

- The protocol is flexible and efficient. Since it is designed for a highly reliable physical medium (fiber optic cable), it may be unsuitable for some tactical media. The ATM could operate over a low bandwidth medium. The two major areas that might preclude ATM from use in the tactical environment are:
  - ATM may be inefficient in sending short cells over a medium in which synchronization is difficult, such as combat net radio. Further, the short cell size could require multiple short messages when a more optimal length would be more efficient.
  - The ATM error detection and correction capability may be inadequate. There is an eight-bit cyclic redundancy check for the header and a separate ten-bit cyclic redundancy check for the user information field. Only a single bit for forward error correction capability on the header as well as on the user information is provided.
- There is no provision within ATM for precedence and preemption; however, these features could be achieved at higher layers over ATM.
- ATM would be reasonably efficient for real-time communication, except that messages requiring multiple cells create the extra overhead of additional transmissions and reassembly.
- Nothing in the ATM addresses security or network management. Network management functions are assumed to take place by the layer or system manager, which has interfaces at each sublayer.
- Nothing in the ATM precludes features such as multimode end-systems or mobile hosts.
- There is no provision for multi-peer data transmission or multi-casting.

9.6.4 Frame Relay Technology

ITU-TS Recommendation I.122, entitled *Framework for Providing Additional Packet Mode Bearer Services*, introduced a new form of packet transmission that has become one of the

most significant contributions of ISDN work. This new technique is now generally referred to as frame-mode bearer service (FMBS) or frame relay. Like cell relay (ATM) and X.25, frame relay allows multiple logical connections to be multiplexed over a single physical interface. As with cell relay, there is no link-by-link error control or flow control with frame relay. Frame relay has higher overhead than cell relay (due to the variable-length packets of frame relay) and its data rate is limited to about 2 Mbps (whereas cell relay operates at 10-100 Mbps). [Ref. Stallings 1993, pp. 243, 277-278]

ITU-TS has published the following frame relay recommendations:

- I.223.1—*ISDN Frame Mode Bearer Services (FMBS) - ISDN Frame Relaying Bearer Services*
- I.223.2—*ISDN Frame Mode Bearer Services (FMBS) - ISDN Frame Switching Bearer Service*
- I.370—*Congestion Management for the ISDN Frame Relaying Bearer Service*
- I.372—*Frame Relaying Bearer Service Network-to-Network Interface Requirements*
- I.501—*Frame Mode Bearer Services (FMBS) Interworking.*

Work on frame relay in the United States uses a data rate of 1.544 Mbps, with future growth to 45 Mbps. ANSI has developed three draft standards [Ref. Stallings 1993, p. 243]:

- T1.606—*Architectural Framework and Service Description for Frame-Relaying Bearer Service*
- T1.617—*Signalling Specification for Frame Relay Bearer Service*
- T1.618—*Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service.*

Frame relay specifications cover two major areas: call control and user data transfer. Frame relay connections may be permanent, in which case call control is not required. For switched frame relay connections, a separate call-control connection is used, providing efficient out-of-band signalling. The data transfer of frame relay specification calls for a two-layer protocol architecture, the physical and data link layers. End-system addressing and connection multiplexing are done at Layer 2. [Ref. Stallings 1993, p. 269]

The key areas in which frame relaying differs from a conventional X.25 packet-switching service are the following [Ref. Stallings 1993, p. 245]:

- Call-control signalling is carried on a separate logical connection from user data. Thus, intermediate nodes need not maintain state tables or process messages relating to call control on an individual per-connection basis.
- Multiplexing and switching of logical connections takes place at Layer 2 instead of Layer 3, eliminating one entire layer of processing.

The protocol architecture for frame relay is based on two separate planes of operations: a control (C) plane, which is involved in the establishment and termination of logical connection, and a user (U) plane, which is responsible for the transfer of user data between subscribers. Thus, C-plane protocols are between a subscriber and the network, whereas U-plane protocols provide end-to-end functionality. [Ref. Stallings 1993, p. 246]

For the actual transfer of information between end users, the U-plane protocol is Q.922. Only the core functions of Q.922 are used for frame relay. The core functions of Q.922 in the U-plane constitute a sublayer of the data link layer. This provides the bearer service of transferring data link frames from one subscriber to another, with no flow-control or error control. Above this, the user may choose to select additional data link or network layer end-to-end functions. In the

control plane, Q.922 is used to provide a reliable data link control service, with error control and flow control, for the delivery of I.451/Q.931 messages. [Ref. Stallings 1993, p. 247]

Because of the simplicity of the frame relay protocol, there are no mechanisms for traditional data link error and flow control. Thus, a frame-relay network is vulnerable to congestion. To compensate for this, simple congestion avoidance and congestion recovery mechanisms are built into the protocol. [Ref. Stallings 1993, p. 269]

9.7 Network Layer Standards

The purpose of the Network Layer is to provide a means for network service users to communicate without any concern for the topology of the network and the transmission media used in each constituent subnetwork that constitute the network. The Network Layer achieves this by performing functions such as routing and relaying. Due to a variety of networking technologies and complex configurations of subnetworks, the operation of the Network Layer is very complicated, sometimes involving the use of more than one network protocol. The network protocols for interconnection are based on the Internal Organization of the Network Layer (IONL) model. The routing protocols are based on the OSI Routing framework, which is specified in ISO/IEC TR 9575 and provides a framework to partition the routing functions. [Ref. Tang 1992, p. 107]

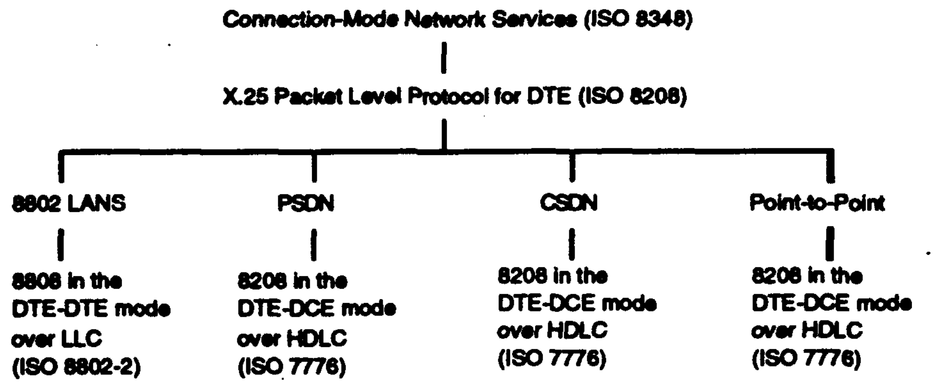
General standards for the Network Layer are listed in Table 19. There are two modes of network services [Ref. Tang 1992, p. 107]:

- Connection-oriented network service (CONS)—the connection-oriented exchange of data that provides for connection establishment, data transfer, and connection termination (as with all connection-oriented services); receipt confirmation, expedited *data, and quality of service*
- Connectionless-mode network service (CLNS)—that connectionless exchange of data that supports actions such as discarding data units, duplicating data units, and delivering data units in a different order than the order in which they were presented by the user. In addition, these services can be optionally qualified as follows: objects will be discarded only after a stated time, objects must be discarded no later than a stated time, objects will be discarded only if more than a certain number of objects are in the queue, objects will not be discarded, the order of the objects in the queue will not be changed, and objects will not be duplicated.

Table 19. General Standards for the Network Layer

ISO 8348	Network Service Definition, Edition 2
ISO 8648	Internal Organization of the Network Layer, February 1988
ISO/IEC 8880-1	Protocol Combination to Provide and Support the OSI Network Service, Part 1: General Principles
ISO/IEC 8880-2	Protocol Combination to Provide and Support the OSI Network Service, Part 2: Provision and Support of the Connection-Mode Network Service
DAM 1	Addition of the ISDN Environment
PDAM 2	Addition of the PSTN and CSDN Environments
ISO/IEC 8880-3	Protocol Combination to Provide and Support the OSI Network Service, Part 3: Provision and Support of the Connectionless-Mode Network Service
WD 8880-4	Protocol Combination to Provide and Support the OSI Network Service, Part 4: Interconnection of OSI Environments
ISO/IEC TR 9577	Protocol Identification in the OSI Network Layer
ISO/IEC TR 10172	Network/Transport Protocol Interworking Specification
ISO/IEC 10177	Intermediate-System Support of the OSI Connection-Mode Network Service Using ISO 8208 in Accordance with ISO 10028
ISO/IEC 10733	Elements of Management Information Related to OSI Network Layer Standards [SC21 N 5560, SC6 N 6413]
WD 10778	High-Speed Integrated Services Networks and User/Network Interface to High-Speed Integrated Services Networks
DIS 11577	Network Layer Security Protocol
ITU-TS T.70	Network-Independent Basic Transport Service for the Telematic Services
ITU-TS X.213	Network Service Definition for OSI for CCITT Applications
ITU-TS X.300	General Principles and Arrangements for Interworking Between Public Data Networks, and Between PDNs and Other Public Networks
ITU-TS X.301 Rev 1	Description of the General Arrangement for Call Control Within a Subnetwork and Between Subnetworks for the Provision of Data Transmission
ITU-TS X.302	Description of the General Arrangement for Internal Network Utilities Within a Subnetwork and Immediate Utilities Between Subnetworks for the Provision of Data Transmission Services
ITU-TS X.305	Functionalities of Subnetworks Relating to the Support of the OSI Connection-Mode Network Service
ITU-TS X.310	Procedures and Arrangements for DTE Accessing Circuit Switched Digital Data Services Through Analogue Telephone Networks
ITU-TS X.320	General Arrangements for Interworking Between ISDNs for the Provision of Data Transmission Services
ITU-TS X.321	General Arrangements for Interworking Between Circuit Switched Public Data Networks (CSPDNs) and ISDNs for the Provision of Data Transmission Services
ITU-TS X.322	General Arrangements for Interworking Between Packet Switched Public Data Networks (PSPDNs) and CSPDNs for the Provision of Data Transmission Services
ITU-TS X.323	General Arrangements for Interworking Between PSPDNs
ITU-TS X.324	General Arrangements for Interworking Between PSPDNs and Public Mobile Systems for the Provision of Data Transmission Services
ITU-TS X.325	General Arrangements for Interworking Between PSPDNs and ISDNs for the Provision of Data Transmission Services
ITU-TS X.326	General Arrangements for Interworking Between PSPDNs and Common Channel Signalling Network (CCSN)
ITU-TS X.327	General Arrangements for Interworking Between PSPDNs and Private Data Networks for the Provision of Data Transmission Services

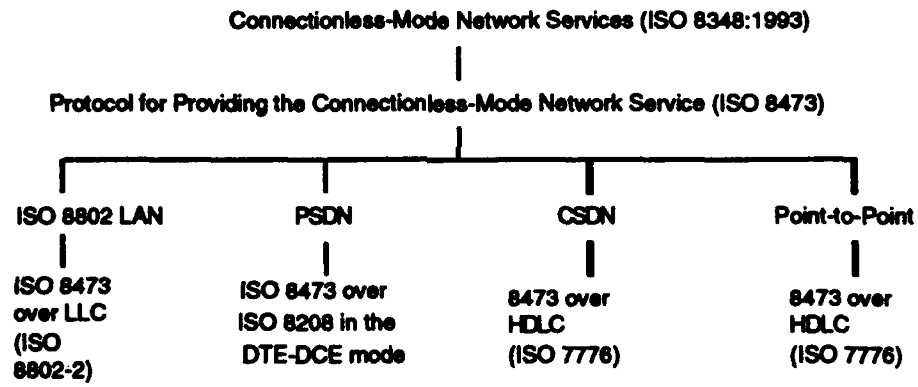
ISO 8880-2 specifies the protocols that are to be used to support the connection-mode network service over a variety of subnetworks. This is illustrated in Figure 9. This protocol is an extension of X.25 that allows both DTE-DTE and DTE-DCE modes of operation. In effect, every type of subnetwork is converted to an X.25 subnetwork, and the virtual circuit capability is used to provide network connections. [Ref. Stallings 1993, p. 103]



Source: [Stallings 1993, p. 104].

Figure 9. Connection-Oriented Mode Network Service

ISO 8880-3 specifies the protocols that are to be used to support the connectionless-mode network service over a variety of subnetworks. Key standards are shown in Figure 10; a complete list of Network Layer standards is provided in Section IV of Appendix D. The network protocol can be used across a single subnetwork. However, the protocol was specifically designed to provide a connectionless internetworking capability that would ride on top of a variety of subnetwork protocols. [Ref. Stallings 1993, p. 103]

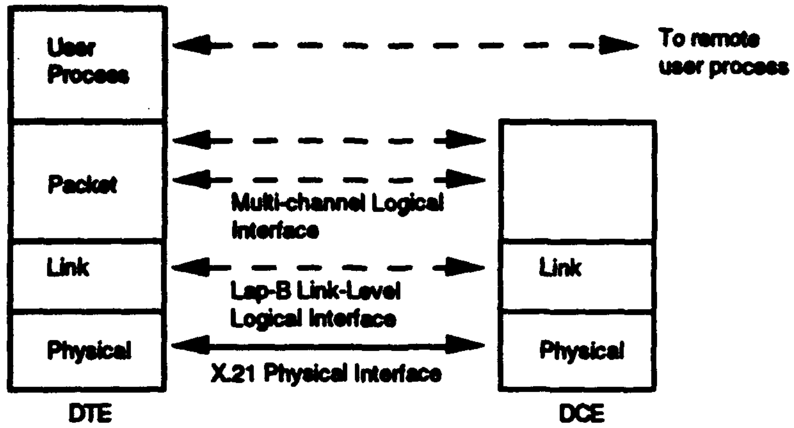


Source: [Stallings 1993, p. 104].

Figure 10. Connectionless-Mode Network Service

9.7.1 X.25 Packet Layer

The X.25 packet-switched network access standard was originally approved in 1976 and subsequently has been revised in 1980 and 1984. This standard specifies a DTE-DCE interface. In the case of X.25, the DCE provides access to a packet-switched network. The standard specifies three levels as illustrated in Figure 11: physical level, link level, and packet level. [Ref. Stallings 1993, p. 113]



Source: [Stallings 1987, p. 113].

Figure 11. X.25 Packet-Switched Network Access Standard

For the physical level the standard is X.21 and optionally X.21 bis. The link level makes use of LAPB over a single physical link between DTE and DCE, and optionally there may be multiple physical links between a DTE and its DCE. The packet level specifies a virtual-circuit service. A compatible version of the packet-level standard has been issued by the ISO (ISO 8208). [Ref. Stallings 1987, p. 113]

The virtual circuit service of X.25 provides for two types of virtual circuit: virtual and permanent virtual call. The virtual call is a dynamically established virtual circuit using call setup and call clearing procedure. A permanent virtual circuit is a permanent, network-assigned virtual circuit. Data transfer occurs as with virtual calls, but no call setup or clearing is required. [Ref. Stallings 1987, p. 114]

Control packets include a virtual circuit number, a packet type identifier, and additional information pertinent to the particular control function. Standards for X.25 packet switching are listed in Table 20. [Ref. Stallings 1987, p. 117]

9.7.2 Connection-Oriented Network Protocol

The connection-oriented network protocol (CONP) is designed to meet the following requirements of internetworking service [Ref. Tang 1992, p. 108]:

- The details of an internetworking operation and the subnetwork facilities should be transparent to the network service users.
- The networking service should allow two communicating network service users to negotiate on QoS and other options during connection establishment.
- The network service users should have a uniform and unambiguous way to address each other using some network addressing scheme.

Peer network service users such as transport entities use a confirmed service element (N-CONNECT) to set up a network connection. During connection establishment, the expedited data selection, the receipt confirmation selection, and the QoS parameters are negotiated. The expedited data selection parameter is used to determine whether expedited data can be sent in the network connection. The receipt confirmation selection parameter is used to determine whether a sender can solicit acknowledgment for some data units. This parameter is particularly useful when the underlying subnetworks are unreliable. Both the expedited data and the receipt confirmation are optional features that do not have to be implemented by the service provider. Within the

constraints imposed by the services of the intervening subnetworks, the network service provider tries to provide the requested QoS. Some of the QoS parameters such as throughput and transit delay are subnetwork dependent while others such as protection and priority are not. [Ref. Tang 1992, p. 108]

Table 20. Standards for X.25 Packet Switching

ISO 8208+	X.25 Packet Level Protocol (PLP) for DTE
AM 1	Alternative Logical Channel Number Allocation
PDAD 2	Extensions for Private Switched Use
AM 3	Static Conformance Requirements
ISO 8878	Use of X.25 to Provide the OSI Connection-Mode Network Service
ISO 8878-2	Use of X.25 to Provide the OSI Connection-Mode Network Service, Part 2: Protocol Implementation Conformance Statement (PICS)
ISO/IEC 8881	Use of the X.25 Packet Level Protocol (PLP) in Local Area Networks
ISO 8882	X.25-DTE Conformance Testing, Part 1: General Principles
DIS 8882-1	X.25-DTE Conformance Testing, Part 1: General Principles, Edition 2 of ISO 8882
ISO/IEC 8882-2	X.25-DTE Conformance Testing, Part 2: Data Link Conformance Test Suite
ISO/IEC 8882-3	X.25-DTE Conformance Testing, Part 3: Packet Level Conformance Test Suite
ISO/IEC 10588	Use of the X.25 PLP in Conjunction with X.21/X.21 bis to Provide OSI CONS
ISO/IEC 10732	Use of the X.25 PLP to Provide OSI CONS Over Telephone Network
ITU-TS X.25	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit
ITU-TS X.75	Terminal and Transit Call Control Procedures and Data Transfer System on International Circuits Between PSDNs
ITU-TS X.223	Use of X.25 to Provide the OSI Connection-Mode Network Service for CCITT Applications (see ISO 8878)
ITU-TS X.244	Procedure for the Exchange of Protocol Identification During Virtual Call Establishment on Packet Switched Public Data Networks
ITU-TS X.612	Provision of the OSI Connection-Mode Network Service by Packet Mode Terminal Equipment Connected to an Integrated Services Digital Network (ISDN) for CCITT Applications

CONS can also be provided over a LAN. In a LAN environment where every DTE is attached directly to the transmission medium, there is no identifiable DCE and thus communication of Layer 2 or above is DTE-to-DTE oriented. ISO/IEC 8881 defined a protocol to enhance the service of LLC2. Essentially this protocol specifies the use of X.25 in the DTE-to-DTE mode in a LAN environment. In the DTE-to-DTE mode, a call request packet and an incoming call are practically the same, and a call accepted packet and a call connected packet are also practically the same. [Ref. Tang 1992, p. 110]

9.7.3 Connectionless Network Protocol

The connectionless network protocol (CLNP) (ISO 8473) is a subnetwork independent convergence protocol, providing the network service over a well-defined set of underlying capabilities that need not be based on the characteristics of any particular subnetwork. CLNP assumes minimal services from the underlying subnetwork, which may be connection-oriented or connectionless. CLNP may run on top of a LAN or a WAN. The protocol data unit used by CLNP is called an internet protocol (IP) datagram, which can contain user data of up to 64 kbytes. [Ref. Tang 1992, pp. 110-125]

9.7.4 Internet (TCP/IP) Standards

The US military has developed and widely implemented (e.g., in the Defense Data Network) unique Internet protocols for Layers 3 and 4 that are not OSI conformant. These protocols will serve as a costandard for the US DoD until transition to OSI is complete. These protocols are identified since they will be implemented in the transition strategy for tactical data systems to be fielded in the 1990s by the US Army. [Ref. Army 1989] Details are provided in Chapter 17. A connection-oriented transport service (COTS) is provided by the Transmission Control Protocol (TCP), which provides end-to-end reliability, and a connectionless-mode network service is provided by the Internet Protocol (IP). The IP provides connectivity over diverse network technologies. Appendix H provides a list of the standards for TCP/IP, including the US military standards (MIL-STDs) and the requests for comment (RFCs).

Historically, TCP/IP arose to meet the need for reliable transmission of information over media that did not guarantee reliable, error-free delivery of information (e.g., Ethernet, Packet Radio, and Satellite). The Defense Advanced Research Projects Agency (DARPA) sponsored research into survivable multi-media packet networking in order to improve the only then-existing network, ARPANET. This research resulted in the US DoD sponsored Internet suite of protocols.

TCP/IP corresponds to Layers 3-4 of the OSI model. In terms of network service, the closest comparison is between the connectionless network service (CLNS) and the service offered by the IP. While the services offered by the OSI CO-mode TP4 and the TCP are similar, three major differences exist:

- The TCP service is stream-oriented, whereas the OSI transport service is packet-oriented.
- The TCP service offers a graceful release, whereas the OSI offers this release in the session service.
- The TCP has an urgent data facility, whereas the OSI has an expedited data service.

One of the commonly used protocols for the Internet is the Point-to-Point Protocol (PPP). The PPP is defined by the following Internet RFCs:

- RFC 1171, *Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-to-Point Links*, July 1990
- RFC 1172, *The Point-to-Point Protocol (PPP) Initial Configuration Options*, 1990
- RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*, November 1992.

The major emphasis of the Internet suite is on the connection of diverse network technologies (Layers 1-4). In addition, several applications for use in the Internet suite are available (see Appendix H; for a more complete listing see [Ref. Reynolds 1987]):

- Simple Mail Transfer Protocol (SMTP)
- File Transfer Protocol (FTP)
- TELNET
- Domain Name System (DNS)
- Simple Network Management Protocol (SNMP) (see Section 12.1.9).

These services are the analogs of MHS, FTAM, VT, Directory, and CMIP, respectively. All of the Internet application protocols are rather simple. They offer a basic level of service and have a very narrow scope. The OSI applications are, in general, functionally more capable than the corresponding applications in the Internet suit. [Ref. Rose 1990] In fact, the US Government, as

well as manufacturers and users, endorse OSI rules at the upper layers while preserving the established TCP/IP networks for the transport of information. [Ref. OSN 1990h] Observers at the INTEROP 90 Conference and Exhibition held in San Jose, California, in October 1990 noted a shift away from pure TCP/IP topics in contrast to the previous year where strongly divided feelings about the merits of OSI versus TCP/IP were revealed [Ref. OSN 1990g]. Until recently, TCP/IP has been a de facto UK standard. However, an IS notice [Ref. CCTA 1991] issued by the UK Central Computer and Telecommunications Agency (CCTA) of HM Treasury included an annex entitled *Towards Open Systems: TCP/IP to OSI Migration*, which provided a Statement of Direction for use by UK Government Departments:

> *It is an inevitable consequence of the move to utilize open systems standards that UK Government departments, in common with other European Public Sector procurement agencies, require the communications and network products that they procure to conform to relevant OSI standards. Departments are therefore advised to make the relevant OSI standards a mandatory condition of a procurement for communications systems where the availability of appropriate standards and products can be confirmed. However, where such availability is questionable, conformance to relevant OSI standards will probably be made a desirable option, but tenders that incorporate OSI standards-based solutions will be viewed as a more acceptable solution in any evaluation of "OSI versus TCP/IP" bids.*

IBM's networking and distributed computing strategy into the next century includes a long-term commitment to the de facto TCP/IP alongside the de jure OSI standards. Originally, it saw TCP/IP as a short-term stop-gap until OSI became more established. However, since OSI took off more slowly than IBM expected, TCP/IP has been established as a long-term option. [Ref. OSN 1992]

The September 1992 issue of *OSN: The Open Systems Newsletter* includes various expert viewpoints on the TCP/IP versus OSI debate.

The technical body that oversees the development of the Internet suite of protocols is termed the Internet Architecture Board (IAB). The IAB is composed of senior researchers, the majority of whom are the designers and original implementors of the Internet suite. Any member of the Internet community can design, document, implement, and test a protocol for use in the Internet suite. The IAB requires that protocols be documented in the RFC series.

There are four RFCs that define the status of documents in the RFC series. The first is the *Assigned Numbers* [Ref. Reynolds 1987], which lists the assigned values used for the parameters in the Internet suite of protocols. The second is *Official Protocols*, which lists all official protocols. The third is *Gateway Requirements*, which lists all protocols and practices that relate to network nodes. And the fourth is *Host Requirements*, which lists all protocols and practices that relate to host nodes. These RFCs are periodically updated, with the most recent document always taking precedence. A list of RFCs is provided in Appendix H.

The migration from the TCP/IP Internet to an OSI/CLNP internet that would be compliant with US GOSIP (see Section 16.1.3.1), international GOSIPs (see Sections 16.1.3 to 16.1.5), and IGOSS (see Section 16.1.3.3) is not well defined (see Sections 9.13.8, 16.1.8, and 19.11.2). Potentially two separate Internets could exist. A proposal for a single protocol framework, called Internet 2000, has been developed to achieve a single Worldwide Internet and avoid two Internets. The framework is a descriptive architecture that is intended to lead to a prescriptive set of

progressive steps and interface definitions facilitating "anything over anything" interworking. Key elements of the proposed framework are the following:[44]

- Continue current practice for subnetworks. TCP/IP Internet and GOSIP are already compatible, in that the TCP/IP Internet does not specify subnetwork technologies and GOSIP recommends a specific set of these technologies.
- Continue to address the "large flat routing table problem" in the TCP/IP Internet by those approaches that would achieve a worldwide CLNP Internet "dialtone" such as TCP over CLNP (TUBA) and Class C supernets (classless interdomain routing, CIDR). Further, worldwide internet service providers should provide CLNP Network Service Access Point (NSAP) addresses in a new Internet worldwide hierarchy to facilitate routing. For transition, newer TCP/IP Internet hosts should implement TCP over CLNP in addition to IP, and older hosts should automatically be assigned new Internet NSAP addresses for use when a CLNP capability is added. Note: CONS is addressed in the proposal as an annex in that it is a feature of GOSIP, EPHOS, and IGOSS but not viewed as a main issue for a single Internet "dialtone."
- Adopt the following three recommendations for Transport services:
  - The TCP/IP Internet should continue to provide TCP and User Datagram Protocol (UDP, equivalent to CLTP) services at Sockets and Transport Library Interface (TLI) interfaces (de facto standard APIs to the Transport service); US GOSIP should continue to provide the OSI CO and CL transport services at XTI (X/Open Transport Interface—an OSI de facto standard API defined by X/Open) interfaces using TP4 and CLTP; and the X.500 Directory should be used to identify the type of Transport protocol entity bound to each NSAP address.
  - RFC 1006, TCP/OSI Coexistence Stack (i.e., TP0 over TCP) should be accepted and extended by defining all the ways that Application services from either suite may call upon Transport services from the other suite—"anything over anything interworking."
  - For the long term (but before 2000), both communities should work together to develop the next-generation Transport protocol using rate-based and selective-retransmission Transport technology that will be needed to run over high-speed, mostly reliable networks such as frame relay, SMDS (connectionless cell switching), and BISDN.
- Maintain the separate methods of providing Application services (direct interface in the TCP/IP Internet for FTP, TELNET, etc.; and use of Session, Presentation, and Application Layers in OSI), with the expectation that OSI will continue to look into how to streamline its upper layers (e.g., a fully recursive Upper Layer Architecture that, like the Network Layer, is basically one layer with a specified three-layer internal organization, together with use of the "OSI skinny stack"). Continue work on new application protocols. The ISO/ITU-TS standardization process should increasingly take account of the principles and methods of the Internet standardization process. To promote application portability, both communities should continue to support development and use of consortia-defined OSEs, APIs, and protocols.

In July 1992, JTC1/SC6 agreed to offer a formal liaison to the IAB to encourage future convergence between the two protocol sets. Two factors make convergence attractive to both groups. The Internet expansion in the market has shown up its technical weaknesses, while the technically superior ISO protocols still lag in market share. If successful, the convergence would focus work on a single approach, saving development costs, support costs, and network costs, as

[44] The GOSIP Institute, *Internet 2000: A Protocol Framework to Achieve a Single Worldwide TCP-IP/OSI/CLNP Internet by Year 2000*, Version 2.2, 11 August 1992. Provided to the 14-17 December 1992 NIST-sponsored OIW meeting on OSE in Gaithersburg, Maryland, as document OSE-TC/92.051.

well as allowing more diverse portable interworking software. [Ref. OSN 1992n] Further, [Ref. SC21 N 7845 1993] contains the Internet Structure and Working Group Summary. There is also a proposal for SC21 to establish a C-liaison with the Internet Society.

9.7.5 Express Transfer Protocol (XTP)

The Xpress Transfer Protocol (XTP) combines the functionality of transport and internet protocols to produce a streamlined protocol that requires minimum processing and allows for parallel processing of some functions. Two types of packet formats are used in XTP: Information packet and Control packet. A common header format and a common trailer format are used for both packet formats, and both header and trailer are of a fixed size to simplify processing. The individual elements of the XTP packets are listed below [Stallings 1991, pp. 609-612]:

- *Route:* Provides the basis for packet forwarding through an internet router. The value is used by a router as an index into a routing table. On each hop, the value in the router field is changed for use by the next router.
- *Time-to-live (TTL):* Maximum remaining lifetime of the packet in the Internet, expressed in 10-millisecond clock ticks.
- *Key:* Logical connection, or context, identifier. It is an end-to-end value generated at one host and communicated unchanged through internet routers to ·· lestination host. Each side of a connection may assign its own key value to the conne ction. Once keys have been exchanged, each side uses the key of the other side in transmissions.
- *Sequence (Seq):* The 32-bit end-to-end sequence number for the context (connection).
- *Rate:* Maximum acceptable transmission rate in octets per second.
- *Burst:* Maximum number of octets receiver will accept per burst of packets.
- *Xkey:* Exchange key. Value ·ssigned to a logical connection by the side that did not originate the connection; the value is returned to the other side for future use.
- *Xroute:* Exchange route. Functions in manner similar to Xkey, for internet routers. In this case, the exchange is done on a hop-by-hop basis, rather than end-to-end.
- *Alloc:* Other side may send octets up to but not including this sequence number.
- *Rseq:* Sequence number expected on next incoming packet; once past the highest consecutive sequence number re·eived without error.
- *Nspan:* Number of pairs in spans array.
- *Spans:* Up to 16 pairs of sequence numbers. Each sequence number pair identifies a span of packets that has been successfully received. This selective acknowledgment identifies gaps of packets that must be retransmitted.

9.7.6 Integrated Services Digital Network

ISDN is the result of the current evolution of the networks and services available from the various PTTs (Post, Telephone, and Telegraph). The original telephone or telegraph networks (PSTNs, Public Switched Telephone Networks) were based on analog equipmen· In recent years, analog equipment has been replaced with digital equipment. This h·· lead to the replacement of analog PSTN with digital IDNs (Integrated Digital Networks). IDN incorporates the latest in digital switching and transmission. The extension of IDN to provide additional user services has resulted in ISDN.

ISDN makes an all-digital interface available to the network subscriber. This system features a high data or bit rate, digital transmission, and digital switching. Digital switching provides a fast connect or call setup for voice and data communications. An ISDN node can connect to packet based and circuit based networks, which can be switched or nonswitched. The

ISDN provides a digital interface to the user. This allows the user to "directly" connect digital devices to the network. The following types of communications channels are used to construct various transmission structures ("pipes"):

- B-channel, 64 kbps—the basic user channel for digital data, digitized voice, and other "mixed" traffic.
- D-channel, 16 or 64 kbps—used to carry signalling information and to set up calls on the B-channels at the customer's interface. The three types of traffic (see below) share the D-channel by means of statistical multiplexing.
- H0-channel, 384 kbps.
- H11-channel, 1.536 Mbps.
- H12-channel, 1.92 Mbps.

Basic access (2B+D) consists of two full-duplex 64-kbps B-channels and a full-duplex 16-kbps D-channel; this 144-kbps information rate has overhead for framing, synchronization, and other requirements that bring the total bit rate to 192 kbps. Reduced variants of basic access are B+D and D alone. Primary access (used for switchboards and LANs) differs for various countries: 1.544 Mbps (the T-1 transmission facility of AT&T) in the United States (typically 23 B-channels plus one 64-kbps D-channel); 2.048 Mbps in Europe (typically 30 B-channels plus one 64-kbps D-channel). Primary rate interfaces using H-channels include: 3H0+D (1.544 Mbps); 4H0 (1.544 Mbps); 5H0+D (2.048 Mbps); 1H1 (1.536 kbps); H12+D (1.920 Mbps); 3H0+5B+D (1.544 Mbps); and 3H0+6B (1.544 Mbps).

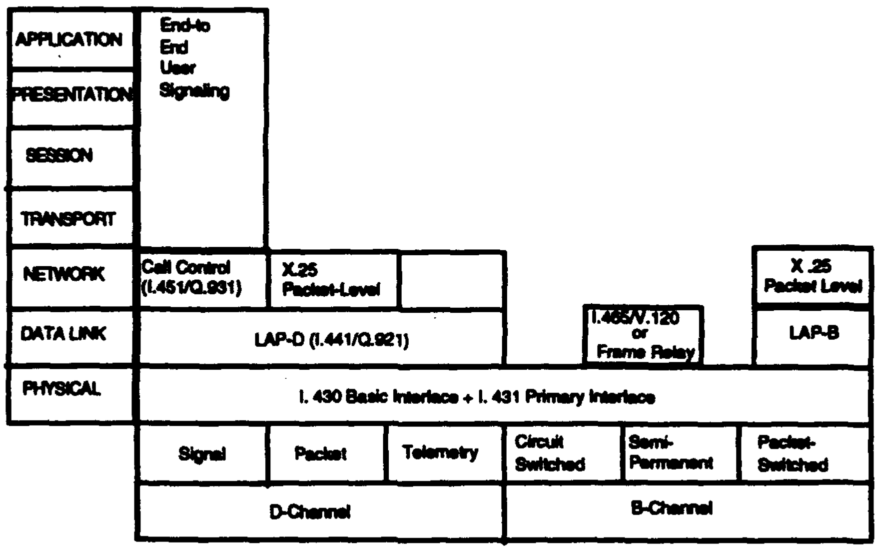
The protocols, services, and interfaces to an ISDN network are defined or specified in the ITU-TS I Series recommendations (see end of Appendix E). ITU-TS SG XVIII is the primary ISDN committee (the ANSI counterpart is the T1S1 committee).

The ISDN protocol architecture is shown in Figure 12, together with the relation of these protocols to the ISO seven-layer model. ISDN is essentially unconcerned with Layers 4 through 7. LAPD is based on HDLC with modifications to meet ISDN requirements for control signaling, packet switching, and telemetry. A link-layer protocol, call control (I.451), supports control signalling by establishing, maintaining, and terminating connections. For packet switching, X.25 packets are transmitted in LAPB frames and the X.25 Packet Level Protocol establishes virtual circuits on the D-channel to other users and to exchange packetized data. The B-channel can be used for circuit switching, semipermanent circuits, and packet switching. In circuit switching, a circuit is set up on a B-channel on demand, using the D-channel call control protocol. Semipermanent circuits are set up using the B-channel by prior agreement; as with circuit-switched connection, the semipermanent circuit (equivalent to a leased line) provides a transparent, full-duplex data path between end systems. Frame relay (see Section 9.6.4) can be used on the B-channel (as well as over H-channels).

Teleservices employ the B-channel for user information and D-channel for signalling information. Teleservices include telephony (3.1 kHz speech); teletex (F.200; end-to-end text communications using standardized character sets, presentation formats, and communications protocols); telefax (Facsimile Group 4 ITU-TS Recommendation; end-to-end facsimile communication using standardized picture coding, resolution, and communications protocols); mixed mode (text and facsimile for end-to-end transfer of documents containing text and fixed images); videotext (provides retrieval and mailbox functions for text and graphic information); and telex (interactive text communication).

The ISDN protocols address several requirements outside the OSI architecture. Examples are the following:

- Multiple related protocols, such as the use of a protocol on the D-channel to set up, maintain, and terminate a connection on the B-channel
- Multimedia calls, allowing a call to be set up that permits information flow consisting of multiple types, such as voice, data, facsimile, and control signals
- Multipoint connections, such as conference calls.



Source: [Stallings 1993, p. 215].

Figure 12. ISDN Protocol Architecture

ITU-TS Recommendation I.430 specifies the physical interface to an ISDN network. It describes the bit, octet, and channel synchronization, as well as the D-channel and access control. Recommendation ITU-TS I.440 describes the data link logical connection via the D-channel. This includes the ability to transfer a packet via the D-channel. This recommendation also indicates how to establish and clear a call through a circuit switched or packet switched network. ITU-TS I.440 and ITU-TS I.441 collectively provide the service and protocol definitions and specifications for an ISDN network.

Recommendations ITU-TS I.450 and ITU-TS I.451 describe how to establish a network connection in a circuit or packet switched network. They describe the protocols for the transfer of a data packet or datagram over a connectionless network. They also describe how to perform the same task using a virtual circuit in a connection oriented network. To allow satellite ISDN connection, work has been undertaken to help ensure compatibility between ITU-TS ISDN recommendations and satellite link parameters [SC21 N 5572, January 1991].

One of the questions for the next (1993-1996) study period proposed by ITU-TS SGVII has to do with the requirements, arrangements, and interface characteristics for the provision of data services in PSDNs when accessed via ISDNs and in ISDNs. [Ref. SC21 N 6956 1992]

To further promote ISDN compatibility and define specific services, a North American (NA) ISDN User's (NIU) Forum has been created with sponsorship of the NIST. It has three objectives:

- Provide a forum for users to influence the developing ISDN to reflect their needs
- Identify ISDN applications and develop implementation requirements for those applications to facilitate timely and interoperable multi-vendor implementations
- Solicit user and product participation in this process.

The NIU Forum consists of two workshops: the ISDN User's Workshop (IUW) and the ISDN Implementor's Workshop (IIW). The IUW produces applications requirements that describe potential applications of ISDN and their requirements. The IIW then develops applications profiles, implementation agreements, and conformance criteria that allow interoperable implementations of solutions to the applications requirements. [Ref. Burr 1991]

ISDN use varies greatly in Europe from nonexistence in some countries to thousands of lines in France and Germany. The European Commission has been actively urging European Community members to implement ISDN services with the goal that by 1994 all member countries will offer commercial ISDN. Some progress is being made toward standardized interconnection between different countries' ISDN services. The first phase of the European Telecommunications Standards Institute (ETSI) calls for all countries' ISDN services to be connected by December 1993; however, to date, a standard has not been developed for such interconnections. [Ref. Computerworld 1991]

According to a recent NIST report on ISDN security [Ref. Burr 1991], ISDN has been developed with little thought to security. The document recommends extending the five security services defined in ISO 7498-2 to all ISDN applications, including voice use of the public network. It contends that a standard for the reliable authentication of human users is badly needed for ISDN security.

The following ETSI profiles specify ISDN-specific protocols (rather than using existing transport and relay profiles for ISDN and the FTAM application profile ISP 10607); when complete, they will be mandatory for nations of the European Commission:

- prETS 300 075, FTAM over ISDN (based on Videotex)
- prETS 300 383, File Transfer over ISDN EUROFILE Transfer Profile, December 1993 (EUROFILE is an ISDN telematic service in which end-to-end compatibility between terminals is guaranteed and which supports file exchanges between different types of equipment; files are exchange over one B-channel at the rate of 64 kbps)
- prETS 300 388, FTAM over ISDN Using Simple File Transfer Standard, December 1993, ETSI.

9.8 Transport Layer Standards

ISO 7498 characterizes the Transport Layer as providing transparent transfer of data between session entities. It relieves session entities from any concern with the detailed way in which reliable and cost-effective data transfer is achieved. All protocols at this layer have end-to-end significance between transport entities in end systems. [Ref. Stallings 1993, p. 175] The Transport Layer standards are listed in Table 21.

The services provided by the Transport Layer can be either in connectionless or connection-oriented modes. ISO has identified five classes of transport protocols. During connection establishment, transport entities negotiate which transport protocol to use based on the QoS

parameter requested by the calling transport service user. This allows implementations of more sophisticated transport protocols to provide a superior service to their users while retaining interoperation with simpler implementations. [Ref. Tang 1992, pp. 29-30]

Table 21. Transport Layer Standards

ISO 8072	Transport Service Definition
AD 1	Connectionless-Mode Transmission
ISO 8073	Connection-Oriented Transport Protocol Specification, Revision
ISO 8602	Protocol for Providing the Connectionless-Mode Transport Service
ISO/IEC TR 10023	A Formal Description of ISO 8072 in LOTOS (awaiting decision concerning further progression)
ISO/IEC TR 10172	Network/Transport Protocol Interworking Specification
PDTR 10734	Guidelines for Bridged LAN Source Routing Operation by End Systems
ISO/IEC TR 10735	Standard Group MAC Addresses
ISO/IEC 10736	Transport Layer Security Protocol
PDAM 1	Security Association Establishment Protocol
ISO/IEC 10737	Specification of Elements of Management Information Related to OSI Transport Layer Standards
ISO/IEC 10740-1	Text and Office Systems - Referenced Data Transfer, Part 1: Abstract Service Definition
ISO/IEC 10740-2	Text and Office Systems - Referenced Data Transfer, Part 2: Protocol Specification
ISO/IEC 11570	Transport Protocol Identification Mechanism
ITU-TS T.70	Network-Independent Basic Transport Service for the Telematic Services
ITU-TS X.214	Transport Service Definition for OSI for CCITT Applications
ITU-TS X.224	Transport Protocol Specification for OSI for CCITT Applications

The definitions of five transport protocol classes depend on the types of network service. ISO identifies three types of network services [Ref. Tang 1992]:

- Type A network service is essentially perfect. The fraction of the packets that are lost, duplicated, or garbled is negligible. Resets are used so rarely that they can be ignored. A point-to-point network is an example of a Type-A network.
- Type B network service provides network connections with an acceptable residual error rate but an unacceptable signalled failure rate. Residual errors are those that are not corrected, and for which transport service provider is not notified. On the other hand, a signalled failure is a failure detected by the Network Layer which then signals the transport entities for recovery.
- Type C network service is not reliable enough to be trusted at all (e.g., the residual error rate is unacceptable). These networks do not detect errors if data are lost, duplicated, re-ordered or corrupted. Transport protocols that must live with Class C network services are most complex of all. A satellite network and an interconnection of LANs and WANs are examples of a Type C network.

The five classes of connection-mode transport protocol, defined by ISO 8073, are based on the three kinds of network services noted above [Ref. Stallings 1993]. The transport protocol classes are the following:

- Class 0. Simple class, oriented for Teletex (upgrade to ITU-TS T.70). Connection flow control is based on network flow control, and connection release is based on release of the network connection.
- Class 1. Basic error recovery class, designed to run on a ITU-TS X.25 network and provide minimal error recovery for network-signalled errors. TPDUs are numbered so that they can be resequenced.

- Class 2. Multiplexing class, an enhancement of Class 0 that still assumes a highly reliable network service. Has the ability to multiplex multiple transport connections onto a single network connection.
- Class 3. Error recovery and multiplexing class. Provides the union of the capabilities of Class 1 and Class 2.
- Class 4. Error detection and recovery class. Assumes that the underlying network service is unreliable, in particular that the TPDUs may be lost or arrive out of sequence. Provides for TPDU retransmission, duplicate detection, flow control, connection establishment and termination, and crash recovery.

9.9 Session Layer Standards

The Upper Layers of the OSI Reference Model are Layers 5-7: Session, Presentation, and Application Layers are handled within ISO/IEC by SC21. Standards in the Application Layer define procedures for the support of distributed information processing. The Application Layer differs from the other layers of OSI in several respects. Entities in the Application Layer are made up of a collection of application service elements (ASEs), each of which is defined by a set of service and protocol standards. These ASEs are combined in various ways to form several types of Application Elements (AEs). The Presentation Layer supports the Application Layer by providing facilities for representing information exchanged between AEs. The Session Layer provides the mechanisms that may be used for controlling interactions between AEs. Standards for the Session Layer are given in Table 22.

Table 22. Session Layer Standards

ISO 8326	Connection-Oriented Session Service Definition (X.215)
AM 4	Additional Synchronization Functionality
WDAM 5	Removal of Session Layer Serial Number Limitation
DIS 8326.2	Connection Oriented Session Service Definition, Edition 2 (X.215)
ISO 8327-1	Basic Connection-Oriented Session Protocol Part 1: Protocol Specification
ISO 8327	Basic Connection-Oriented Session Protocol Specification (X.225)
AM 3	Incorporate Additional Synchronization Functionality
WDAM 4	Removal of Session Layer Serial Number Limitation
DIS 8327-1	Basic Connection-Oriented Session Protocol, Part 1: Protocol Specification, Edition 2 of ISO 8327 (X.225)
ISO 8327-2	Basic Connection-Oriented Session Protocol, Part 2: PICS Proforma (X.245)
ISO 9548	Session Connectionless Protocol to Provide Connectionless-Mode Session Service (X.235)
ISO/IEC 9548-2	Session Connectionless Protocol to Provide Connectionless-Mode Session Service, Part 2: PICS Proforma (X.255)
DIS 10168-1	Conformance Test Suite for the Session Protocol, Part 1: Test Suite Structure and Test Purposes
CD 10168-2	Conformance Test Suite for the Session Protocol, Part 2: Common Session Abstract Test Suite
CD 10168-3	Conformance Test Suite for the Session Protocol, Part 3: Abstract Test Suite for the CS Method
DIS 10168-4	Conformance Test Suite for the Session Protocol, Part 4: Session Test Management Protocol Specification
ITU-TS X.215	Session Service Definition for OSI for CCITT Applications
ITU-TS X.225	Session Protocol Specification for OSI for CCITT Application
ITU-TS X.235	Connectionless Session Protocol (ISO 9548)
ITU-TS X.245	Session PICS Proforma (ISO 8327-2)
ITU-TS X.255	Connectionless Session PICS Proforma (ISO/IEC 9548-2)

The primary purposes of the session service are to organize a session dialogue and to mange the data exchange between two communicating session service users. These purposes are accomplished as follows [Ref. Tang 1992]:

- To organize a session dialogue, the Session Layer adds structure to a transport pipe. A session connection can be structured into activities representing different logical pieces of work. An activity can be structured further into dialogue units. With the use of this structure, the Session Layer provides service elements for activity management and dialogue control. The dialogue control facilities allow a session service user to insert either major synchronization points, which separate dialogue units, or minor synchronization points, which can appear anywhere within a dialogue unit. A resynchronization service is also provided to assist orderly re-establishment of communication.
- To manage the data exchange, the session service provides four kinds of data transfer facilities:
  - Normal data transfer facility, which can operate in either full-duplex or half-duplex mode and for which only the owner of the data token can send data
  - Expedited data transfer facility
  - Typed data transfer facility, which allows a session service user to send data outside the normal data stream independent of the availability and the assignment of the data token
  - Capability data transfer facility, which allows session service users to exchange limited amounts of user data while not within an activity.

In a liaison statement to SC21/WG6, ITU-TS SGVII stated that the concepts of "dependent conformance" and "general conformance" are not sufficiently defined to be used in the Session PICS (ISO 8327-2) now. [Ref. SC21 N 6905 1992]

The ITU-TS Session Layer telematic recommendations are:

- T.5, *General Aspects of Group 4 Facsimile Apparatus*
- T.62, *Control Procedures for Teletex and Group 4 Facsimile Services*
- X.3, *Packet Assembly/Disassembly Facility (PAD) in a Public Data Network (PDN)*
- X.20, *Interface Between DTE and DCE for Start-Stop Transmission Services on Public Data Networks*
- X.28, *DTE/DCE Interface for a Start/Stop Mode DTE Accessing the PAD in a PDN Situated in the Same Directory (Country)*
- X.29, *Procedures for the Exchange of Control Information and User Data Between a PAD and a Packet Mode DTE or Another PAD.*

Conformance Testing standards for the Session Layer include [Ref. SC21 N 8081 1993]:

- DIS 10168-1, *Conformance Test Suite for the Session Protocol* - Part 1: *Test Suite Structure and Test Purposes*, April 1990 (expected to reach IS status by end of 1994)
- CD 10168-2, Part 2: *Common Session Abstract Test Suite* (replaces the former CD 10168-2, *Generic Test Suite*, March 1992, which was cancelled since ISO 9646 no longer recognizes generic test suites)
- CD 10168-3, Part 3: *Abstract Test Suite for the CD Method*, September 1993 [SC21 N 8164] (replaces *Generic Test Suite*, March 1992, which was cancelled since ISO 9646 no longer recognizes generic test suites)
- DIS 10168-4, Part 4: *Session Test Management Protocol Specification*, March 1991 (expected to reach IS status by end of 1994).

9.10 Presentation Layer Standards

The Presentation Layer provides two types of service, one to handle the representation of information exchanged between two communicating application entities so that the types and values of the information exchanged will be preserved, and another that is session related (required by the OSI architecture for session-related requests). General Presentation Layer standards are given in Table 23.

The Presentation Rapporteur Group is requesting comments from National Bodies regarding the merits of adding support for compression of protocol data units (PDUs) within the presentation protocol. Options could include compression of the complete presentation PDU, compression of the complete user data parameter of the presentation PDU, or a selectable transformation to be applied to the encoding of an individual presentation data value. [Ref. SC21 N 6985 1992]

The telematic services for the Presentation Layer are defined by the following ITU-TS recommendations:

- T.6, *Facsimile (FAX) Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus*
- T.51, *Coded Character Sets for Telematic Services*
- T.61, *Character Repertoire and Coded Character Sets for the International Teletex Service*
- T.73, *Document Interchange Protocol for the Telematic Services.*

9.10.1 Abstract Syntax Notation One (ASN.1)

Application entities need to know the structure and content of application protocol data units, but not their representation. Agreeing on a common representation is a responsibility of the Presentation Layer. An abstract syntax language is used to describe the structure and content of a structured object. Encoding rules specify a representation for the physical data exchange. [Ref. Tang 1992]

At present, ASN.1 is the only abstract syntax language that exists in OSI. Abstract syntax languages describe data types in a machine-independent manner, thus freeing data representation from machine restrictions. For example, a protocol specifying that a data type is an integer need not concern itself with the number of bits required for the internal machine-dependent representation of this data type.

ASN.1 has a rich syntax for describing data types and provides a macro facility for extending its grammar. According to Rose [Ref. Rose 1990],

> *ASN.1 is destined to become the network programming language of the 90s, just as the C programming language is largely seen as having been the systems programming language of the 80s.*

The pertinent specifications (December 1987, Revised April 1990) for ASN.1 are ISO 8824, ISO 8824/AD1 (incorporated into ISO 8824), ISO 8824/DAM 2, ISO 8824/PDAM 3.2, and recommendation X.208 from ITU-TS. The ISO specifications are compatible with those of ITU-TS, but include a few extensions. [Ref. Stallings 1987]

Table 23. General Presentation Layer Standards

ISO 8822	Connection-Oriented Presentation Service Definition (X.216)
AM 1	Connectionless-Mode Presentation Service
AM 2	Unlimited User Data
DAM 3	Abstract Syntax Registration
AM 4	Support of Session Symmetric Synchronization Service
AM 5	Delivery of Additional Session Synchronization Functionality to the Presentation Service User
DIS 8822.2	Basic Presentation Service Definition, Edition 2
ISO 8823	Connection-Oriented Presentation Protocol Specification (X.226)
AM 2	Unlimited User Data
DAM 3	Transfer Syntax Registration
AM 4	Support of Session Symmetric Synchronization Service
AM 5	Additional Synchronization Functionality to the Presentation User
DIS 8823-1	Connection Oriented Presentation Protocol, Part 1: Protocol Specification, Edition 2 of ISO 8823
ISO/IEC 8823-2	Connection-Oriented Presentation Protocol Specification, Part 2: Presentation Protocol Implementation Conformance Statement (PICS) Proforma (X.246)
ISO 9576	Presentation Connectionless Protocol to Provide Connectionless-Mode Presentation Service (X.236)
DIS 9576-2	Presentation Protocol to Provide the Connectionless-Mode Presentation Service, Part 2: PICS Proforma for Connectionless Presentation Protocol (X.256)
ISO/IEC 10729-1	Conformance Test Suite for the Presentation Protocol, Part 1: Test Suite Structure and Test Purposes
DIS 10729-2	Conformance Test Suite for the Presentation Protocol, Part 2: Test Suite for ASN.1 Encodings and Test Purposes for Presentation Protocol
WD 10729-3	Conformance Test Suite for the Presentation Layer, Part 3: Common Presentation Abstract Test Suite
ITU-TS X.216	Presentation Service Definition for OSI for CCITT Applications
ITU-TS X.226	Presentation Protocol Specification for OSI for CCITT Application
ITU-TS X.236	Connectionless presentation protocol (ISO 9576)
ITU-TS X.246	Presentation PICS Proforma, (ISO 8823-2)
ITU-TS X.256	Connectionless Presentation PICS Proforma, (ISO 9576-2)

ASN.1 standards are listed in Table 24. The table shows that the current ISO 8824 is being revised as Part 1 of a four-part standard arranged as follows:

- Part 1: *Basic Notation*
- Part 2: *Information Object Specification* —provides notation that allows information object classes as well as individual information objects and sets thereof to be defined and given reference names.
- Part 3: *Constraint Specification*—describes how the notation can be defined that further constrains the values that can appear in the notation of Parts 1 and 2, which define a structured data type to convey their semantics.
- Part 4: *Parameterization of ASN.1 Specifications*—describes how specifications may leave certain aspects (e.g., bounds) undefined at the time of abstract syntax definition, being completed by the specification of ISPs for functional profiles from some other body. The requirements not met by Parts 2 and 3 are met in Part 4 by the provision for parameterized reference names and parameterized assignments by this part of the ASN.1 specification.

ASN.1 Information Objects, Constraints, Parameterization - Tutorial and Worked Examples, Version 2, May 1991, provides a tutorial and collection of worked examples related to the proposed ASN.1 extensions in the area of macro replacement. Its aim is to support the early adoption of these extensions by current macro users. [Ref. SC21 WG6 N 1171 1992]

Table 24. Presentation Layer ASN.1 Standards

ISO/IEC 8824	Specification of Abstract Syntax Notation One (ASN.1) (X.208)
DAM 2	Amendments to ISO 8824 to Give ISO 8824 Part 1: Specification of Basic Notation
WDAM 4	Removal of Definition of Root Arcs of Object Identifier Tree
ISO/IEC 8824-1	Specification of Abstract Syntax Notation One (ASN.1), Part 1: Specification of Basic Notation (X.680)
PDAM 3.2	Rules of Extensibility
ISO/IEC 8824-2	Specification of Abstract Syntax Notation One (ASN.1), Part 2: Information Object Specification (X.681)
ISO/IEC 8824-3	Specification of Abstract Syntax Notation One (ASN.1), Part 3: Constraint Specification (X.682)
ISO/IEC 8824-4	Specification of Abstract Syntax Notation One (ASN.1), Part 4: Parameterization of ASN.1 Specifications (X.683)
ISO/IEC 8825	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) (X.209)
DAM 2	Amendments to ISO 8825 to Give ISO 8825 Part 1: Basic Encoding Rules
AM 3	Rules for Extensibility
DIS 8825-1	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 1: Basic Encoding Rules (BER) (X.690)
WDAM 1	Light Weight Encoding Rules for ASN.1
DIS 8825-2.2	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 2: Packed Encoding Rules (PER)
DIS 8825-3	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 3: Distinguished and Canonical Encoding Rules (X.692)
DIS 8825-4	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 4: Test Suite Structure and Test Purposes for ASN.1 Encodings
SC21 N 6130	Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression
ITU-TS X.208	Specification of Abstract Syntax Notation One (ASN.1)
ITU-TS X.209	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)
ITU-TS X.680	ASN.1 Specification, Basic ASN.1 (ISO 8824-1)
ITU-TS X.681	ASN.1 Specification, Information Object Specification (ISO 8824-2)
ITU-TS X.682	ASN.1 Specification, Constraint Specification (ISO 8824-3)
ITU-TS X.683	ASN.1 Specification, Parameterization (ISO 8824-4)
ITU-TS X.690	ASN.1 Specification, Basic Encoding Rules (ISO 8825-1)
ITU-TS X.692	ASN.1 Specification, Distinguished/Canonical Rules (ISO 8825-3)

Material on an Abstract Syntax Model [SC21 N 6133, December 1991] was removed from the ASN.1 Enhancements as being too immature at this stage. However, it is believed that the topic requires further consideration. Other topics that require further consideration include ASN.1 compatibility issues [SC21 N 6134, January 1992] and application indexes [SC21 N 6135, January 1992].

The Framework for the Support of Distributed Applications (DAF), a new activity established by ITU-TS SG VII to standardize common aspects of distributed applications, has been working for various enhancements to ASN.1 with the following goals [Ref. OSN 1990f]:

- Provide a firmer framework for the specification of table types and functions
- Improve current definitions of character strings
- Provide new encoding rules—Packed Encoding Rules (PER), Confidential Encoding Rules (CER), Lightweight Encoding Rules (LWER), and Distinguished Encoding Rules (DER)—to supplement or replace the current Basic Encoding Rules (BER)
- Improve machine processability
- Provide miscellaneous enhancements.

SC24/WG1 is developing an Image Processing and Interchange (IPI) Standard (see Section 7.2.2.4) that is noted in ASN.1; however, several questions have arisen requiring liaison with

SC21/WG6. One important issue is the apparent inefficiency of representing large arrays that are fundamental to the expression of image data. [Ref. SC24 N 744 1992]

9.10.2 ASN.1 Encodings

The mechanism that translates the abstract representation of data to its physical characteristics, either for machine storage or for transmittal, is called transfer syntax. The transfer syntax in OSI corresponding to the abstract syntax ASN.1 is contained in *Basic Encoding Rules,* ISO 8825. The relevant standards for BER are ISO 8825, ISO 8825/AD1, ISO 8825/AD2, and ITU-TS X.209. Again, the ISO and the ITU-TS specifications are compatible.

Additional sets of encoding rules are being incorporated into ISO/IEC 8825 by making the current standard Part 1 and developing a revised ISO/IEC 8825, *Specification of Encoding Rules for Abstract Syntax Notation One (ASN.1),* into a multi-part standard as follows:

- DIS 8825-1 (Part 1): *Basic Encoding Rules (BER),* 1993
- DIS 8825-2.2 (Part 2): *Packed Encoding Rules (PER),* 1993 [SC21 N 7302]
  - WDAM 1, *Lightweight Encoding Rules,* August 1993 [SC21 N 7920]
- DIS 8825-3 (Part 3): *Distinguished and Canonical Encoding Rules*, October 1992 [SC21 N 7213] (SC21 has requested its Secretariat to conduct an national body default ballot proposing that the text of DIS 8835-3 be merged into the text of DIS 8825-1 [Ref. SC21 N 8081 1993])
- DIS 8825-4 (Part 4): *Test Suite Structure and Test Purposes,* July 1990 [SC21 N 5019].

There is a requirement for an upper layer international standard or recommendation to specify a "quality of service," which implies that the use of transfer syntaxes will provide, within the upper layers, a high level of security, including features for confidentiality and integrity. This specification defines a generic transfer syntax whose use is negotiated by the presentation protocol or announced in an ASN.1 external. It provides a generic transfer syntax that can be applied to any abstract syntax defined using ASN.1. [Ref. SC21 N 6130 1991] The new work item was accepted provisionally by JTC1 with a request that SC21 reevaluate the need for the project, the wording of the scope, and the effort required for progress on the project. Several national bodies have raised concerns regarding the benefits to be derived from progression of the project [SC21 N 6604, December 1991]. *Generic Transfer Syntax Providing Upper Layers Security*[45] is currently in WD form.

The BER use a "TLV" approach to mapping between abstract and physical data wherein each data type is encoded as a Tag, a Length, and a Value. The tag field corresponds to the label defined by the data type's abstract syntax, the length field normally indicates how many octets are used for the encoding of the value portion of the data type, and, finally, the value of the data type is encoded.

PER achieve a more compact representation than that achieved by the BER. For each value the CER select just one encoding from those allowed by the BER, eliminating all of the sender's options. LWER encode and decode data much faster than the BER.

FIPS 121, *Videotext/Teletext Presentation Level Protocol Syntax,* adopts ANSI X3.110-1983 (with the same title) as the specific data syntax to be used at the presentation layer (and some

[45] The title given to this document at the May/June 1991 meetings in Arles was *Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression.*

specific semantics for the application layer) for videotext and teletext applications. It is based on the American National Standard Code for Information Interchange (ASCII) and its extensions. FIPS 121 provides formats, rules, and procedures for the encoding of alphanumeric text and pictorial information to be used with broadcast television videotext service.

ITU-TS Recommendations F.200, S.60, S.61, S.62, and S.70 define the service, the terminal equipment, character repertoire, control procedures, and supporting transport services for Teletex. ITU-TS Recommendation X.430 (Red Book 1984) describes the access protocol for Teletex Terminals.

A new standard, ASC X3.208-199x, *Transfer Syntax Description Notation (TSDN)*, is being developed by ANSI X3.T2. It defines a notation for describing the structures of data volumes, files, records, and fields to facilitate the moving of data files between computer systems. While it provides a generalized syntax for describing the data records, it does not restrict or define their contents. It was originally developed as an internal standard by the Consultative Committee on Space Data Systems (CCSDS) to handle the transmission of space data. [Ref. Freeman 1991] It is currently in draft form.

9.11 Application Layer

The Application Layer is at the boundary between the open systems environment and the application processes that use that environment to exchange data. To support the wide variety of possible applications, the protocols and services potentially available in the Application Layer are many and varied. They include facilities of general utility to a wide variety of applications and facilities specific to distinct classes of applications.

The Application Layer directly serves applications by providing the required communication support. A communication component of an application—an application entity—communicates with a peer application entity using an application protocol. Some application protocols involve only two objects or systems, while others involve more. Application protocols are described using information models, which describe how a class of information structures is organized.

9.11.1 Common Upper Layer Requirements (CULR)

The Session, Presentation, and Application Layers share a number of requirements. Standards for the upper layers considered together are the following:

- ISO/IEC 10745, *Upper Layer Security Model*, November 1993 [SC21 N 8334] (X.803)
- pDISP 11188-1, *Common Upper Layer Requirements*, Part 1: *Basic Connection-Oriented Requirements*, July 1993
- pDISP 11188-2, *Common Upper Layer Requirements*, Part 2: *ROSE-Based Requirements*, July 1993
- pDISP 11188-3, *Common Upper Layer Requirements*, Part 3: *Minimal OSI Upper Layer Facilities*, July 1993
- DIS 11586-1, *Generic Upper Layer Security (GULS)*, Part 1: *Overview, Models and Notation*, October 1993 [SC21 N 8182] (X.830)
- DIS 11586-2, *Generic Upper Layer Security (GULS)*, Part 2: *Security Exchange Service Element (SESE) Service Definition*, October 1993 [SC21 N 8183] (X.831)

- DIS 11586-3, *Generic Upper Layer Security (GULS)*, Part 3: *Security Exchange Service Element (SESE) Protocol Specification*, October 1993 [SC21 N 8184] (X.832)
- DIS 11586-4, *Generic Upper Layer Security (GULS)*, Part 4: *Protecting Transfer Syntax Specification*, October 1993 [SC21 N 8185] (X.833)
- WD 11586-5, *Generic Upper Layer Security (GULS)*, Part 5: *Security Exchange Service Element (SESE) - PICS Proforma*, June 1993 [SC21 N 7912] (X.834)
- WD 11586-6, *Generic Upper Layer Security (GULS)*, Part 6: *Protecting Transfer Syntax - PICS Proforma*, June 1993 [SC21 N 7913] (X.835).

Upper Layer Security Model. The purpose of the Upper Layer Security Model is to provide standards developers with the architectural model for the development of application-independent services and protocols for security in the upper layers of OSI and the use of these services and protocols to fulfill the security requirements of a wide variety of applications, so that the need for application-specific ASEs to contain internal security services is minimized. This standard provides detail of the positioning of and the interaction between security services in the upper layers; describes the handling of security transformation functions (e.g., encipherment) and security check-value functions from the Application and Presentation Layer; introduces the concept of a security exchange; addresses security policy and security state; and broadly discusses the provision of entity authentication, data origin authentication, association access control, resource access control, non-repudiation, integrity, and confidentiality. The relationship of the Upper Layer Security Model to other security standards is provided in the *Guide to Open Systems Security*, December 1993 [SC21 N 8380].

Common Upper Layer Requirements (CULR). pDISP 11188 is a multi-part ISP that specifies general requirements on the use of OSI connection-mode protocols by application profiles. The CULR does not contain the definition of any complete profiles but is intended to be referenced normatively by other ISPs that define application profiles. The CULR provides common text for such ISPs or other referencing specifications, simplifying the specification process on facilitating common implementation of the protocols for use in different application profile contexts.

Generic Upper Layers Security (GULS). The GULS standards define a set of generic facilities to assist in the provision of security services in OSI applications. These include the following [Ref. SC21 N 8380 1993]:

- A set of notional tools to support the specification of (1) selective field protection requirements in an abstract syntax specification, (2) security exchanges, and (3) security transformations
- Service definition, protocol specification, and PICS proforma for an application service element, *Security Exchange Service Element (SESE)*, to support the provision of security services in the Application Layer
- A specification and PICS proforma for a security transfer syntax that is associated with Presentation Layer support for security services in the Application Layer.

GULS specializes some of the Application Layer concepts of the Upper Layer Security Model. It should be viewed as only a starting point for upper layers security, as it lacks any specifics on how particular classes of mechanisms may be used to support generic security requirements. Its tools address security transformations (e.g., encryption, digital signatures) as required for confidentiality, integrity, data origin authentication, and possibly non-repudiation. [Ref. DRA 1994]

9.11.2 Application Layer Structure (ALS)

ISO 9545, *Application Layer Structure (ALS)*, was originally published by ISO in December 1989. In 1993, a new version, with extended ALS (XALS, ISO 9545:1993) was published. ISO 9545 defines the nature of standards in the Application Layer and the relationships among them, the architectural framework in which individual OSI Application Layer protocols shall be developed, and the categories of identifiable objects that are necessary for the specification and operation of protocols. It also relates distributed information processing activities to the standards in the Application Layer. Key concepts from the ALS are the following:

- Association (application association)—a cooperative relationship between two AE invocations for the purpose of communicating information and coordinating their joint operation. This relationship is formed by the exchange of application protocol control information using the Presentation Service.
- Application context—a set of rules shared in common by two service element (SE) invocations in order to enable their cooperative operation. The application context is an example of a shared conceptual schema. SC21 N 5502 is a liaison to ITU-TS Q23/VII concerning application context negotiation during association establishment. Other relevant references include:
  - *Guidelines for Application Context Definition* [SC21 N 6071]
  - *Discussion Paper on Application Context Negotiation* [SC21 N 6122]
  - *A Possible Approach for Application Context Negotiation During Association Establishment* [SC21 N 6123].
- Single association object (SAO)—the collection of things in an AE invocation related to a single application association.
- Single association control function (SACF)—the component of a single association object that represents the use of those rules in the application context concerning interactions among ASEs within a single application association.
- Multiple association control function (MACF)—a component of the AE invocation that coordinates the interactions among multiple associations within an AE invocation in order to provide a coordinated service.

The purpose of XALS is to supplement ISO 9545 by providing a more complete framework for development of Application Layer protocol standards that use other Application Layer protocol standards. A central focus of XALS is extension of the architecture for use of multiple associations. [Ref. SC21 N 4901 1990] The text, which was approved in March 1993, is in SC21 N 7815. It is formatted as a revision to the ALS standard (ISO 9545:1993) intended for publication as a new edition, not as an amendment. The new edition offers greater power and flexibility than the first edition. It includes a multi-level structure and more on control function and ASO-type specification. [Ref. SC21 N 7817 1993]

XALS provides a revised ALS model that is significantly richer in scope and descriptive capability than is provided in ISO 9545. As a result, it provides more options for the specification of Application Layer standards. Examples of new features are:

- Defining Application Service Elements (ASEs), application service objects (ASOs), and control functions. An ASO is made up of one or more ASEs and/or ASOs, and a control function. A control function is the component of an ASO that controls the interactions among ASEs and/or ASOs within the containing ASO.
- Providing guidance for ASE specifications in the areas of the reference model the ASE supports, the service definition, the abstract protocol definition, and the ASE environment requirements specification.

- Addressing peer-to-peer (application level) relationships as well as the established concept of application association, such as are used on MHS, TP, EDI, and Directory.
- Accommodating both peer-to-peer and client-server interaction styles. (ROSE supports both styles of interaction. X-Windows and DOAM use client-server styles, for which the terminal in the X-Window environment is the server, whereas the terminal in the DOAM model is the client.)

As a result of using the XALS model, the UK believes that there is a need to provide some guidance to those groups that are making use of it in their modelling and specification of Application Layer functions. In particular, there is a need for guidance on how to develop ASE and ASO specifications that may be used in a variety of AE configurations. This is because there are conflicts in the ASE specification regarding their assumptions about the use of supporting services such as ACSE and Session Resynchronization. Moreover, there are cases of both overlapping and conflicting functionality. The United Kingdom therefore proposes to amend the ASE specifications to achieve compatibility and produce a specification for the combination of the ASEs. [Ref. SC21 WG6 N 1155 1992]

An amendment to ISO 9545 for connectionless mode transmission has been in the working draft stage since 1988 and has lacked an editor and target dates. In June 1993, the project was cancelled.

Methodology and Guidelines for the Development of Application Layer Protocols, January 1990, is being developed to provide a discipline for development of application protocol standards in order to generate precise specifications. It is now a working draft [SC21 N 8410].

A question concerning Versions and Extensibility [SC21 N 6060, May 1991] of the ALS has come to the attention of SG6. Variants of Application Layer protocols may arise for a number of reasons; for example, a protocol may be revised to support additional capabilities or to provide different capabilities. It is important to ensure that Application Layer protocols are designed so as to enable implementations of different variants to co-exist and interwork (where feasible) and, equally importantly, to provide an environment that facilitates the orderly migration from one network systems configuration to another. SC21 N 6965, June 1992, the revised draft answer to this question, was approved in October 1992.

SC21 N 6967 *Modelling Recovery in the Application Layer*, June 1992, ISO 9545 WDAM 2 adds to concepts and principles of ISO 9545 by categorizing the nature of failures visible in the Application Layer and defining the concepts and modelling principles for recovery. Target dates are CD in July 1993, DIS in July 1994, and IS in July 1995. It is to be merged with ISO 9545:1993.

9.11.3 Application Service Elements (ASEs)

The services performed in the Application Layer of the OSI model can be thought of as application processes whose communication aspects are represented by application entities. The OSI Application Layer structure permits an application process to have multiple communication aspects and, hence, multiple application entities.

An application entity is a collection of one or more ASEs. Each of the peer application entities have identical ASEs. Additionally, each ASE talks only with its peer in the remote application entity. The remainder of this section discusses the following ASEs (the SESE was described in Section 9.11.1 above):

- Association Control Service Element (ACSE), which provides association control and manages connections between application entities
- Commitment, Concurrency, and Recovery (CCR), which provides fault tolerance and manages error indication and recovery
- Reliable Transfer Service Element (RTSE), which manages bulk data transfers
- Remote Operations Service Element (ROSE), which manages request/reply interactions
- Remote Call Procedure (RPC)
- User ASE defined in Transaction Processing.

A typical application process might have a user element orchestrating the application entities' actions. This user element could use RTSE services to manage associations via ACSE services and could use the ROSE, which invokes RTSE services, to transfer data through the use of the presentation service.

9.11.3.1 Association Control Service Element (ACSE)

The ACSE is defined for the purpose of managing application associations. It provides facilities for the establishment and release of application associations. An application association is a presentation connection with additional application layer semantics such as application context negotiation and peer-to-peer authentication. At present, there is a one-to-one mapping between application associations and presentation connections. However, future versions of the ACSE standard might permit a presentation connection to be reused for a new association or multiple associations to be interleaved onto a single presentation connection. Because the sole purpose of ACSE is to manage application associations, ACSE does not provide any data transfer service elements. Thus, in any application context containing ACSE, there are one or more user-ASEs that will provide some data transfer service elements. [Ref. Tang 1992]

The ACSE provides service to both user elements and to specific application service elements. The purpose of this service is to support the establishment, maintenance, and termination of application associations. Because the ACSE manages the association of application entities, all OSI applications contain an ACSE. The services provided by ACSE are:

- ASSOCIATE, which sets up an application association
- RELEASE, which releases an association in an orderly fashion
- ABORT, which terminates application association simultaneously with the underlying presentation and session connections.

The ISO definition of the service is technically aligned with the 1988 ITU-TS recommendation on the ACSE service. The differences between the ISO definition and the ITU-TS definition are quite small and are not expected to affect interoperability between implementations written against either document. [Ref. Rose 1990] SG7 of ITU-TS is progressing the second editions of the ACSE Protocol and Service while SC21 has not. The texts approved by ITU-TS differ from the texts of record in SC21, however, the differences are believed to be editorial. [Ref. SC21 N 7868 1993] SC21 has recently begun work on second editions to ISO 8649 and 8650.

The relevant ISO standards are the following:

- ISO 8649, *Service Definition for the Association Control Service Element (ACSE)*, April 1992 (X.217)
  - DAM 3: *Application Context Negotiation During Association Establishment* [SC21 N 8046, September 1993]
- DIS 8649.2, *Service Definition for the Association Control Service Element (ACSE)*, Edition 2 (IS expected November 1994)
- ISO 8650, *Protocol Specification for the Association Control Service Element (ACSE)*, April 1992 (X.227)
  - DAM 2: *Application Context Negotiation During Association Establishment* [SC21 N 8047, September 1993]
  - WDAM 3: *A-Context Management Service* (DAM expected June 1994; AM expected June 1995)
- DIS 8650-1, *Protocol Specification for the Association Control Service Element (ACSE)*, Edition 2 (IS expected November 1994)
- ISO 8650-2, *ACSE, Part 2: PICS Proforma* (X.247)
- ISO/IEC 10035, *Connectionless ACSE Protocol Specification* (X.237)
- DIS 10035-2, *Connectionless ACSE Part 2: PICS Proforma*, September 1993 [SC21 N 7870 rev.] (X.257) (initiation of ITU-TS approval expected November 1994)
- ISO/IEC 10169-1, *Conformance Test Suite for the ACSE Protocol, Part 1: Test Suite Structure and Test Purposes*, September 1991 [SC21 N 6421].
- WD 10169-2, *Conformance Test Suite for the ACSE Protocol, Part 2: Common ACSE Abstract Test Suite* (project risks cancellation by SC21 in the absence of written confirmation that the regional workshops will provide a WD by June 1994). [Ref. SC21 N 7728 1993])

A discussion paper [SC21 N 5835] on association pools as an extension of ACSE appeared in April 1991. The United States then requested that WG6, in collaboration with TP and RPC, consider extending ACSE to provide support for facilities of XALS and Application Pools. The project would generate amendments to ACSE service definition and protocol (ISO 8649 and 8650) specification to support XALS and Association Pools. WD status was proposed for June 1993, CD for June 1994, and DIS for January 1995. [Ref. SC21 N 6798 1992]

In June 1992, SC21 accepted an NP for Extension to ACSE Covering ASOs and ASO-associations. The amendments to ISO 8649 and 8650 will add extensions in two areas:

- ASO addressing extension to the existing A-ASSOCIATE service
- Providing a standardized way to establish and release ASO-associations.

WDAM was planned in November 1992, PDAM in July 1993, DAM in July 1994, and AM in July 1995. [Ref. SC21 N 7014 1992] Although this NP has met the criteria for acceptance into the JTC1 program of work, several national bodies question the user requirements for this new work item (NWI). SC21/WG8 (formerly WG6) is requested to respond to the comments received. [Ref. SC21 N 7723 1993]

9.11.3.2 Commitment, Concurrency, and Recovery (CCR)[46]

The CCR service and protocol standards are used to supply a more fault tolerant association than is possible with ACSE. The ACSE has two basic flaws [Ref. Stallings 1987]:

[46] Portions of this section are excerpted from [Tang 1991].

- A system crash leaves ambiguous results.
- A lack of coordination of multiple systems could produce inconsistent results.

These flaws are resolved in CCR by adding the concept of commitment. The master asks the subordinate for a commitment to perform a task (request) before the call for the execution of the task (commitment) is made. This allows for a record to be kept by both the master and the subordinate as to the status of the task. Use of CCR can have an adverse performance impact.

Concurrency is a concept that is necessitated by the concept of commitment. Once an application entity has offered to commit, conflicting requests cannot be made against the application until the commitment is fulfilled. Concurrency is the mechanism by which committed resources are "frozen" until the committed application is completed.

Recovery is the process of determining the status of a task after an application or communication failure. The CCR service provides partial support for recovery; however, the actual recovery process is specific to the application.

The CCR standard (ISO 9805) provides the communication mechanism for the two-phase commit protocol on a single application association between two CCR service users. It provides the CCR service users with service primitives to commit, rollback, and recover from failures. It does not provide any data transfer facilities. Therefore, the CCR-ASE must be used with one or more user-ASEs that can supply the data needed for an atomic action.

The CCR ASE provides a set of service elements to coordinate two AEs involved in an atomic action. An atomic action is a well-defined set of operations that has four properties: atomicity, consistency, isolation, and durability (ACID). The atomicity property means that, to an *outside observer*, either all of the operations are completed or none of them is executed. The consistency property means that the operations are performed correctly with respect to the application semantics. The isolation property means that any partial results of the operations composing the atomic action are not accessible before the completion of the atomic action. Finally, the durability property means that the action must endure a communication or an application failure.

To preserve the ACID properties, the two-phase protocol taken from database theory is used. This protocol ensures that the state is remembered prior to any work, so that an earlier consistent state can be recreated if the work is damaged. (The notion of recreating an earlier state is called rollback.) CCR supports the communication aspects of the two-phase protocol. For example, a CCR service user can use CCR service elements to request its peer to offer commitment, to signal to its peer that it is ready to commit, and to command a peer to rollback or to initiate recovery.

Bound data refers to the data whose state may be affected by an atomic action. The two-phase protocol makes sure that the modification of the bound data is done indivisibly. Commitment releases bound data in the final state while rollback releases bound data in the initial state.

Atomic action data consists of state information about an atomic action. When a communication or an application failure occurs, a CCR service user relies upon the atomic action data to perform recovery. CCR uses the presumed rollback recovery mechanism. For this mechanism, the subordinate acquires the recovery responsibility when it decides to offer commitment, while the superior acquires the recovery responsibility when it decides to order commitment.

There are three standards relating to CCR:

- ISO/IEC 9804, *Service Definition for the Commitment, Concurrency, and Recovery Service Element* (X.851)
- DIS 9804.2, *Service Definition for the Commitment, Concurrency, and Recovery Service Element,* Edition 2 (ballot closed November 1993)
- ISO/IEC 9805, *Protocol Specification for the Commitment, Concurrency, and Recovery Service Element* (X.852)
- ISO/IEC 9805-1, *Protocol Specification for the Commitment, Concurrency, and Recovery Service Element,* Edition 2 of ISO/IEC 9805
- DIS 9805-2.2, *Protocol Specification for CCR, Part 2: PICS Proforma.* (X.853) (IS status expected September 1994).

ISO/IEC 9804 and ISO/IEC 9805 have three amendments: *Enhancements, Session Mapping Changes (Additional Synchronization Functionality),* and *Restart.* Amendment 1 for each has reached PDAM status, and Amendment 2 has reached AM status.

In January 1990, a CCR *Conformance Test Suite* was proposed as a new work item [SC21 N 4279]. CD status was expected in June 1992. This project risks cancellation by SC21 in the absence of written confirmation that the regional workshops will provide a WD by June 1994.

Another new work item [SC21 N 6126] has been accepted for writing a formal description of the CCR service and protocol using LOTOS. WG6 has developed PDTRs for a *LOTOS Description of the CCR Service,* PDTR 11589, June 1993 [SC21 N 7876] and *Protocol,* PDTR 11590, June 1993 [SC21 N 7877].

9.11.3.3 Reliable Transfer Service Element (RTSE)

RTSE provides a service of reliably moving arbitrarily large objects from one application entity to another. The RTSE accomplishes this service by dealing with ASN.1 data types rather than a string of octets and by abstracting the complexity of the underlying service session into an easily usable service.

If a network failure occurs while a bulky application protocol data unit (APDU) such as a large file or a long message is transferred over a wide area network, then the entire APDU may have to be retransmitted. RTSE ensures that the APDU, whatever its size, is transferred exactly once or that the sender is warned of an exception. RTSE provides such service through the use of the session service. To the RTSE users, RTSE provides a simple reliable transfer facility by hiding the complexity of the session service. The RTSE standard, as specified in ISO/IEC 9066, is primarily used by MHS. Formerly called RTS (Reliable Transfer Server), RTSE is used to regulate and control mail transfer between local and remote MTAs. In particular, it is used by the P1 protocol over a wide area network. When sending mail over a reliable LAN, the overhead incurred by RTSE cannot not be justified, hence RTSE is not used. [Ref. Tang 1992]

When an application context contains an RTSE, it is the sole user of ACSE services and the presentation service. The RTSE is used to signal to application elements that a transfer has been completed successfully. The ISO standard for RTSE comes in two parts with a third under development:

- ISO/IEC 9066-1, *Reliable Transfer,* Part 1: *Model and Service Definition* (X.218)
- ISO/IEC 9066-2, *Reliable Transfer,* Part 2: *Protocol Specification* (X.228)
- DIS 9066-3, *Reliable Transfer,* Part 3: *PICS Proforma* (X.248) [SC21 N 7677, March 1993] (initiation of ITU-TS ballot expected June 1995).

Since RTSE was developed in the early MHS work that preceded the definition of the presentation service and ULA, it demands syntax conversions be done in the Application Layer (rather than in the Presentation Layer as specified by the ULA). Thus, RTSE does not fit well with the OSI ULA. [Ref. SC21 N 5997 1991]

9.11.3.4 Remote Operations Service Element (ROSE)

Remote operations are a popular technique for building distributed applications. The ROSE manages operations for application entities via a mechanism that is analogous to services performed by CCR for data transfer. ROSE provides the facilities to invoke a remote operation on another computer, to have the result of the operation or an error message returned to the invoker, or to have the remote operation rejected as invalid [IGOSS 1993].

ROSE provides the communication support for a typical request-reply interaction. In an application context containing ROSE, there are one or more user-ASEs that supply the requests or replies in the form of remote operations to ROSE. On receiving a remote operation, the ROSE protocol constructs a ROSE APDU and sends it using either RTSE or the presentation service. The ROSE service definition provides service elements to invoke an operation, to return a result/reply, or to reject the execution of an operation. It also supports the use of linked operations. For example, using the linked operations feature, a management agent can link multiple replies to a single request from a manager. Before a ROSE user can invoke any operation, it must first register a set of remote operations with the ROSE service provider even before an application association is made with a peer. At the time of application association establishment, it must specify whether the application context should contain RTSE or not. [Ref. Tang 1992]

In its most primitive form, an operation is a simple request/reply interaction. The request, or invocation, consists of:

- An operation number—a unique identifier for the operation to be performed
- An arbitrarily complex argument—the "input" for the operation
- An invocation identifier—a unique identifier for a particular invocation
- A linked invocation identifier—an indication that this operation is being invoked as a part of the processing of another invocation.

An invocation can have one of three outcomes:

- A result—an invocation identifier corresponding to the operation that succeeded and an arbitrarily complex result
- An error—an invocation identifier corresponding to the operation that failed, an error number uniquely identifying the error that occurred, and an arbitrarily complex parameter that provides clarifying information
- A rejection—an invocation identifier corresponding to the operation that was performed and a reason that describes the rejection that occurred.

The standards that apply to the ROSE are:

- ISO 9072-1:1989, *Remote Operations*, Part 1: *Model, Notation and Service Definition*, Revised Edition, September 1989 [SC21 N 3881] (X.219)
  - PDAM 1, *Enhancements to Service Definition*, April 1992 [SC21 N 6717] (to JTC1 for endorsement to cancel the project)
- ISO/IEC 9072-1:1993, *Remote Operations*, Part 1: *Concepts, Model and Notation*, Edition 2, March 1993 [SC21 N 7669] (passed DIS ballot in October 1993) (X.219) (see DIS 13712-1)
  - PDAM 1, *Built-In Operations*, June 1993 [SC21 N 8073]

- ISO/IEC 9072-2:1989, *Remote Operations*, Part 2: *Protocol Specification*, Revised Edition, September 1989 [SC21 N 3882] (X.229)
  - PDAM 1, *Enhancements to Protocol Specification*, April 1992 [SC21 N 6718] (to JTC1 for endorsement to cancel the project)
- ISO/IEC 9072-2:1993, *Remote Operations*, Part 2: *Service Definition*, Edition 2, March 1993 (passed DIS ballot in October 1993) [SC21 N 7670] (see DIS 13712-2)
  - PDAM 1, *Mapping to A-UNITDATA and Built-In Operations*, July 1993 [SC21 N 8074]
- ISO/IEC 9072-3:1993, *Remote Operations*, Part 3: *Protocol Specification*, March 1993 (passed DIS ballot in October 1993) [SC21 N 8074] (see DIS 13712-3)
  - PDAM 1, *Mapping to A-UNITDATA and Built-In Operations*, June 1993 [SC21 N 8075]
- DIS 9072-4, *Remote Operations*, Part 4: *PICS Proforma*, December 1993 [SC21 N 7678] (initiation of ITU-TS approval ballot expected November 1994) (X.249) (see DIS 13712-4)
- DIS 13712-1, *Remote Operations*, Part 1: *Model*, 1993 (X.880) (initiation of ITU-TS ballot approval February 1994) (see 9072-1)
  - PDAM1, *Built-In Operations*, January 1994 [SC21 N 8406]
- DIS 13712-2, *Remote Operations*, Part 2: *Service*, 1993 (X.881) (initiation of ITU-TS ballot approval February 1994) (see 9072-2)
  - PDAM1, *Mapping to A-UNITDATA and Built-In Operations*, January 1994 [SC21 N 8407]
- DIS 13712-3, *Remote Operations*, Part 3: *Protocol*, 1993 (X.882) (initiation of ITU-TS ballot approval February 1994) (see 9072-3)
  - PDAM1, *Mapping to A-UNITDATA and Built-In Operations*, January 1994 [SC21 N 8408]
- DIS 13712-4, *Remote Operations*, Part 4: *PICS Proforma*, 1993 (X.883) (initiation of ITU-TS ballot approval November 1994) (see 9072-4)
- WD 13712-5, *Remote Operations*, Part 5: *Enhancements*, 1993 (initiation of ITU-TS ballot approval June 1995).

ROSE is a set of communications facilities to distributed applications. ROSE was derived from the Remote Operations (RO) service defined in ITU-TS MHS-84. The standard (ISO 9072) also provides a notation for defining them (an extension of ASN.1). Remote operations service is asynchronous, so a client need not wait for a response before invoking another operation. ISO 9072 defines the structure of remote operations and the abstract services and protocol to support them. The services are generic in that their effect on the remote object is defined by their users.

The basic interaction with a remote object is an operation that is similar to a procedure call in a programming language. An operation is invoked on a target object, to which the operation argument is passed. Operations have one of two possible structures, and invocations have two possible outcomes. Some operations return either a Result, when they are executed successfully, or an Error; other operations produce only a response (Error) if the operation fails.

The emerging four-part revision of ROSE covers only a subset of extensions that are needed. For successful collaboration between JTC1 and ITU-TS on ROSE, it was necessary for SC21 to propose yet another NWI [SC21 N 7013] in May 1992 [Ref. SC21 N 6719 1992], which received adequate National Body support to be forwarded to JTC1 for NP letter ballot. The NP would enhance the three-part ROSE specifications [SC21 N 6716-6718] through amendments to include the:

- Addition of built-in operations for optional inclusion in any application context
- Mapping of ROSE APDUs onto the A-UNITDATA service
- Addition of various QoS fields in ROSE information objects and new information object classes for specifying QoS.

PDAM status was achieved in March 1993. DAM is expected in February 1994 and AM in February 1995. [Ref. SC21 N 7013 1992]

9.11.3.5 Remote Procedure Call (RPC)

RPC extends the local procedure call to a distributed environment. In a RPC, a process can invoke a remote procedure as if it were invoking a local procedure. By hiding the communication details from the invoking process, RPC promotes applications portability. RPC is extremely useful for distributed applications. For example, a client application involving a computationally complex procedure can use RPC to have that procedure run on a remote high speed computer. This will improve the throughput of the application dramatically. Since RPC only defines a style of interaction, it can be combined with any OSI application standard that leaves the data transfer facilities open to the users. For example, it can be used with the OSI Transaction Processing standard. Since TP does not provide a method for transferring data, it is up to a TP application to determine its own envelope. [Ref. Tang 1992]

The RPC standard specified a RPC computational model and a RPC engineering model. The RPC computational model describes the style of program interaction, while the RPC engineering model describes the protocol used to support the RPC computational model. Before a client can request a service from a server, it must first obtain a service reference that includes the location of a server in particular. With the service reference, the client can establish a binding with the server and start invoking services. The trading service provides the means for clients to obtain service references. In general, trading refers to the process of importing, exporting, and matching proposals. [Ref. Tang 1992]

The ECMA standard for RPC is ECMA 127. As defined in ECMA 127, an RPC is a communication service to transfer procedure calls to a remote server and return results, errors, or associated call backs. One of the central notions of RPC is that of a stub. A stub builds protocol information for RPCs (marshalling) and translates protocol information to server procedure calls (unmarshalling). ECMA 127 defines an Interface Definition Notation (IDN) to facilitate the transfer of data across an interface. The IDN supports a union of programming language-specific data types such as pointers, arrays, and records, and primitive data types such as integers and bit strings. ECMA 127 limits the number of outstanding procedure calls to one per association, in order to prevent livelock situations and preserve fairness; it is unclear if this is the most efficient solution to the livelock problem. SC21/WG6 proposes to address RPC using an IDN that is based on abstract data types rather than on a union of programming language-specific data types.

Text for DIS 10148, *Basic Remote Procedure Call (RPC) Using OSI Remote Operations* [SC21 N 3463], was based on ECMA 127 and submitted in 1989 on a fast-track ballot, which failed. DIS 10148 was withdrawn, and a September 1989 proposal for a new work item was accepted by JTC1 in May 1990. The draft standard, DIS 11578, has five parts:

- DIS 11578-1, Part 1, *Model* [SC21 N 8212, September 1993]
- DIS 11578-2, Part 2, *Interface Definition Notation;* uses data types defined by SC22/WG11 and defines a mapping of these to ASN.1 [SC21 N 8213, September 1993]

- DIS 11578-3, Part 3, *Service Definition: Basic RPC ASO Service* [SC21 N 8214, September 1993]
- DIS 11578-4, Part 4, *Protocol Specification: Basic RPC ASO* [SC21 N 8215, September 1993]
- WD 11578-5, Part 5, *PICS Proforma* [SC21 N 6111, June 1991]. (SC21 is considering canceling WD 11578-5 in the absence of an Editor and WD. [Ref. SC21 N 7728 1993])

Some of the work being undertaken in ECMA with respect to RPC includes the following:

- *Position on RPC Modelling* [SC21 N 5816, March 1991]
- *Binding Concepts Within RPC* [SC21 N 5817, March 1991]
- *Proposal for RPC Service Definition and Protocol Specification Parts* [SC21 N 5818, March 1991]
- *Modelling Rationale for OSI RPC* [SC21 N 5819, March 1991]
- *Contribution on Computation Model* [SC21 N 5821, March 1991]
- *Proposal for the Use of XALS in the Standardization of RPC* [SC21 N 5822, March 1991]
- *Position on RPC Context Handles* [SC21 N 5823, March 1991].

ISO work with respect to RPC includes the following:

- *Nature of the OSI RPC Service Boundary and Service Provider* [SC21 N 5586, January 1991]
- *Working Definitions for Client and Server* [SC21 N 5590, January 1991]
- *Call for Comment on OSI RPC IDN* [SC21 N 5588, January 1991]
- *Mapping Between RPC IDN and ASN.1* [SC21/WG6 N 1199, June 1992].

The aim of the current work in ISO on RPC is to provide a mechanism for writing distributed applications that are both syntactically and semantically similar to a local procedure call.[47] The scope of RPC includes a language-independent IDN for specifying interfaces between components of distributed applications. The RPC protocol for a particular interface definition is derived from the IDN.

RPC is closely related to two projects in SC22: Common Language Independent Data Types (CLID) (ISO 11404) and Common Language Independent Procedure Call Mechanism (CLIP or CLIPCM) (see also Section 4.3.1). SC22/WG11 has agreed that there is no overlap between the CLI projects and RPC. However, there should be cross references between the standards. The CLI projects identified below are giving an abstract definition of data types and procedure call mechanism, while RPC is a concrete definition that extends the procedure calls to the distributed environment [Ref. SC21 N 5583 1991]:

- CLID defines a set of data types, independent of any particular programming language specification or implementation. The set should be rich enough so that all common data types in standard programming languages and service packages can be mapped onto some data type in the set. Hence, the CLID standard is an abstract definition of the set of data types in terms of the values a data type can take and some of the operations that are valid on the data type. The ISO RPC standard will define the set of data types it supports, including the presentation of values of these data types when exchanged in parameters of a remote procedure call.

[47] The ISO approach to RPC could be a problem for Ada.

- The aim of CLIP is to define a generic model for procedure call semantics and therefore is an abstract definition of a procedure call mechanism. ISO RPC aims to extend the semantics of a local procedure call in a distributed environment and, in particular, that the RPC be semantically and syntactically similar to a local procedure call.

It is not at all clear whether remote operations (ISO 9072) can be used to satisfy RPC requirements or whether collaborative work with ITU-TS will be conducted for RPC. SC21/WG6 has identified requirements for RPC and IDN and has begun coordination of these requirements with SC22/WG11 and ITU-TS SGVII. [Ref. SC21 N 4926 1990; SC21 N 4928 1990]

In December 1992, the WG8 RPC Group proposed a liaison to SC22/WG11. Specifically, it requested guidance on how best to tackle internationalization in the RPC IDN and for experience and advisability of reserving terminal symbols in programming languages. [Ref. SC21/WG8 N 62 1992] ASN.1 may not be adequate as a basis for the IDN, even if extended for this purpose. Some requirements for the IDN identified in SC21/WG6 are [Ref. SC21 N 4767 1990]:

- Be user friendly in the sense that an applications programmer can translate from the IDN to the programming language of choice in a straightforward, approximately one-to-one manner
- Be usable to automatically generate language-specific interfaces that support procedure calls using the RPC service
- Be usable to automatically generate the programming language-specific procedure declarations that correspond to the procedures in an IDN for use by a server.

There would appear to be some danger of duplication of effort—and possibly even rival standards—unless RPC is brought together, in some manner, with ROSE. [Ref. OSN 1990e] For example, ROSE has already standardized an IDN, called RO-notation, that uses ASN.1 as a language-independent way of describing the data types of the parameters. ROSE is already used widely, and a program of enhancements to allow it to meet additional needs is underway. However, ROSE is not even mentioned in the new RPC work item proposal.

The UK is concerned that the mapping between the RPC IDN and ASN.1 should always produce one and only one ASN.1 type for each RPC interface type definition. This is essential for the correct encoding of data types. Following discussions in the October 1992 RPC Rapporteur meeting, the UK updated the formal mapping rules between the two notations. [Ref. SC21 N 7614 1993]

The Distributed Office Applications Model (DOAM) standards (ISO 10031) have been developed assuming the support of ROSE. In a January 1992 liaison statement to SC21/WG6, SC18/WG4 SWG on DOA requested that RPC be developed in a manner that allows applications in the DOAM framework to exploit compliant RPC implementations without modification. [Ref. SC21 N 6656 1992] In its reply, WG6 stated that use of RPC by existing implementations (e.g., of an application in the DOAM framework) is probably not technically possible. If a standard is to be changed to use RPC rather than ROSE, it must change its interface notation from RO-notation to the RPC IDN. [Ref. SC21 WG6 N 1170 1992]

Two RPC implementations currently exist: Sun RPC and OSF RPC. The two are not mutually exclusive, and the key issue for the user is agreement on the application program interface so the user does not have to worry about differences in various RPCs. This requires a standardized interface definition language such as the Network Interface Definition Language

(NIDL), which was developed by Apollo, is being enhanced by Digital, and is the basis of an ANSI recommendation to ISO. [Ref. OSN 1990g]

9.11.3.6 User Application Service Element

A new ASE is emerging from development of the Distributed Transaction Processing (TP) standard (ISO 10026), just as RTSE evolved from the RTS of ITU-TS X.410. The TP protocol (ISO 10026-3) does not provide an explicit protocol for transmitting user data. The TP service standard (ISO 10026-2) provides a service (TP-DATA) that is implemented by a user application service element (U-ASE). The TP standards specify a general mechanism that allows a set of programs to interact in a controlled manner but, because of its generality, it was not possible for the standard to specify what data would flow between programs (this is in sharp contrast to X.400, in which data flows were standardized). The U-ASE is both separate from and part of the TP program. It is part of the TP program because it is crafted to encode and decode its data stream—a U-ASE made for a specific data stream is useful only to programs that need that data stream. It is separate from a program because it can be used by many programs. A TP program can use two different U-ASEs to communicate with different types of users. [Ref. IGOSS 1993]

9.11.4 Message Handling System (X.400)

9.11.4.1 MHS and MOTIS Overview[48]

The Message Handling Systems (MHS) standard facilitates the exchange of all kinds of information among MHS users through the OSI communication system. Although MHS uses mainly interpersonal messages, the MHS service may be also used to exchange business documents and others. One of the principle features of MHS is its operation in a store-and-forward manner so that the originator's system does not have to be attached to the recipient's system. Instead, the message may be routed via one or more intermediate systems.

CCITT (not ITU-TS) first published the well known X.400 standard in 1984. Since then, ITU-TS and ISO/IEC have worked together to harmonize their activities and produced parallel standards with almost identical text. They are the ITU-TS's X.400 (1988) and the ISO/IEC 10021 Message Oriented Text Interchange System (MOTIS). The differences between the X.400 standard and the MOTIS standard are minor.

The 1988 MHS standard (denoted MHS-84) contains many improvements over the 1984 MHS standards (denoted MHS-88). These improvements include the use of user friendly Directory names instead of user unfriendly originator/recipient addresses to identify MHS users, the use of distribution lists to name groups of recipients, the provision of security services that were practically absent in MHS-84, and the use of the full OSI stack for compatibility with other OSI system software.

A User Agent (UA) provides access to the Message Transfer Service (MTS) or a Message Store (MS) on behalf of its user. It submits and delivers messages for its user. It may provide text processing facilities for the composition of messages. Some UAs are specialized to handle person-to-person communication, some are specialized to handle business documents, and others are for some specialized content type. In general, a UA can only process a certain content type. Currently, only two content types have been standardized: the interpersonal message (IPM) content type and the Pedi (edi standing for electronic data exchange) content type. An IPM content

---

[48] This section has been excerpted from [Tang 1991].

type is used for person-to-person communication, while a Pedi content type is used for business trading. Thus, there are IPM-UAs and Pedi-UAs.

9.11.4.2 Status and Relation of MHS and MOTIS Standards

Table 25 summarizes the set of standards that define MHS (X.400) and MOTIS (ISO/IEC 10021) services. Efforts made by the ITU-TS (formerly CCITT) and ISO to converge MHS and MOTIS resulted in 1988 with sets of standards that are substantially, but not completely, compatible. [Balloting for the previous MOTIS standards (DIS 8505, DIS 8883, and DIS 9065) was suspended, and the scope of these standards has been incorporated in ISO 10021.]

The relationships of the X.400-1984, X.400-1988/1992, and MOTIS (1988 and 1992) standards are also provided in Table 29. Notice that MOTIS still has no parallel to the X.408 standards for algorithms used when converting between different types of encoded information, no parallel for the X.430 (now T.430) Teletex access protocols, and none for X.403.

Table 25. Base Standards for MHS

Layer	X.400-1984	X.400-1988 and X.400-1992	MOTIS
7 7	X.400 X.401	X.400[a]	ISO 10021-1
7	X.400	X.402	ISO 10021-2
7	N/A	X.403[b]	None
7	N/A	X.407	ISO 10021-3
7	X.408	X.408	None
7	X.409	X.208 X.209	ISO 8824 ISO 8825
7	X.410	X.218 X.219 X.228 X.229	ISO 9066-1 ISO 9072-1 ISO 9066-2 ISO 9072-2
7	X.411	X.411 X.419[c]	ISO 10021-4 ISO 10021-6[c]
7	N/A	X.413	ISO 10021-5
7	X.420	X.420 (IPM)	ISO 10021-7
7	X.430	T.430	None
7	N/A	X.435 (EDI) X.440 (Voice) X.4xx (Mgmt)	TBD (new in 1988) TBD (new in 1992) TBD (new in 1992)
7 (ACSE)	N/A	X.217 X.227	ISO 8649 ISO 8650
6	N/A	X.216 X.226	ISO 8822 ISO 8823

Source: Provided originally by OMNICON in September 1988.

[a]1988 X.400 Series is double-numbered with 1988 F.400 Series.

[b]Citation for X.403-1988 (and X.403-1992) includes three manuals.

[c]1988 and 1992 X.419 and ISO 10021-6 have a wider scope than the part of 1984 X.411 and DIS 8883 that they replace.

MHS 1988. MHS 1988 provided new (relative to MHS 1984) capabilities for message store (listing, summary, fetching, and deletion of stored messages); security services (origin authentication, secure access management, data confidentiality, data integrity, nonrepudiation, and security management); distribution lists (members, submit permission, expansion point, and

owner); directory services (authentication, name resolution, data list expansion, and capability assessment); physical delivery service (basic physical rendition, ordinary mail, physical forwarding, and return of undeliverable mail); and conformance testing (methods, criteria, and notation). In addition, MHS 1988 revised MHS 1984 standards for naming, addressing, routing, and special access.

MHS has been extended since 1984 to include voice, EDI, and file transfer in the message body. Also many bugs in the specification have been fixed.

NIST Special Publication 500-182, *Guidelines for the Evaluation of Message Handling Systems Implementations,* details a generic process that helps users acquire MHS. The guide advises how to determine the best MHS for electronic mail requirements, and how to identify potential MHS implementations. Candidate implementations can then be measured against function and performance factors, and rated. [Ref. CSL 1992, p. 2]

An ISO/IEC/ITU-TS Computer Conferencing Working Document is now in Version 13.

A group is working on an "asynchronous group communication" standard based on X.400, X.500, and DFR. This will include a new system similar to but more sophisticated than USENET and facilities for joint editing of documents and voting/polling. The name of the draft standard is currently X.gc.

The MHS 1988 recommendations were supplemented by a new series of standards on the service aspects of MHS. These ITU-TS recommendations are:

- F.400, *System and Service Overview*
- F.401, *Naming and Addressing for Public Message Handling Services*
- F.410, *The Public Messaging Transfer Service*
- F.415, *Intercommunication with Public Physical Delivery Services*
- F.420, *The Public Interpersonal Messaging Service*
- F.421, *Intercommunication Between the IPM Service and the Telex Service*
- F.422, *Intercommunication Between the IPM Service and the Teletex Service.*

MHS 1992. MHS 1992 revises X.402, X.411, X.413, X.419, X.420, and X.435; there are major additions to X.413 and X.420. Two new recommendations are included: X.440, Voice Messaging System; and X.4xx, MHS Management. MHS 1992 enhancements include the following [Ref. PSC 1991]:

- <u>File transfer</u>—allows any kind of files, such as word processing documents, spreadsheets, object programs, and other binary files, to be sent via X.400. Closely aligned with ISO 8571 (FTAM), MHS 1992 caters to store and forward needs rather than direct connection file transfer intended in FTAM. Rather than using a separate content type, file transfer in MHS 1992 is done through a new body part type, which can be used in IPMS and EDI content types. Transfer of binary files in MHS 1992 is based on and compatible with a new recommendation: X.bft, Binary File Transfer for the Telematic Services. T.bft adds a capability to transfer files to T.30 on Group 3 Facsimile and to DTAM protocols (T.bft is technically aligned with FTAM but with some extensions for use in a personal computing environment). Transfer syntax may be ASN.1 BER or as specified by the document type. Transfer of portions of a file or multiple files in MHS is for further study. Files may be compressed before transfer, and the sender may request how the data being transferred is to be used in relation to files to be stored by the recipient. These and other interoperability parameters for MHS file transfer are as follows:

- Content type parameter—indicates the abstract data types of the contents of the file and the structuring information, in order to maintain complete file structure and semantics during transfer
- Compression parameter—describes the compression algorithm by specifying the algorithm identifier and algorithm parameters
- Related stored file parameter—indicates to the recipient any intended relationship (e.g., created, replaced, extended) between the file in this body part and any file(s) held by the recipient
- File attributes parameter—carries the values of any of a set of optional file attributes representing a request to the recipient to use these values if a new file has to be created based on initial file attributes (not all FTAM file attributes are included in MHS)
- Environment parameter—describes the environment (e.g., machine, operating system, application) from which the file originated
- Extensions parameter—conveys the information not accommodated by the other parameters of file transfer body part (has the same syntax and usage as that for the IPM content type extensions field)

• Notifications—provides consistency with P1 Delivery notifications: IPMS to IPMS, IPMS to telematic AUs, and IPMS to facsimile

• Accounting—permits originator, on message submission, to specify reverse charging on a per recipient basis; uses the MHS 1988 extension field mechanism to specify a parameter to say the percentage to be charged to the recipient (e.g., 0 percent); applies only to messages and is critical for submission, which means that systems that do not understand the extension or that do not support the type of charging requested will reject the submission of the message

• Auto-submitted Indication—allows the originator, or enables the User Agent or Message Store, to indicate to the recipient whether the message was or was not automatically submitted by a machine without either the direct or indirect human control over the submission and to determine the nature of the submission; values are not auto-submitted, auto-generated, auto-replied, and auto-forwarded (absence of this indication reveals no information as to whether or not the message submission involved human control)

• P22 Extensions—augments extension "buckets" provided by MHS 1988 to include new per-recipient heading fields and new notifications for the P22 (IPM) protocol, allowing for future extensions but does not include any such actual extensions and retaining the existing P22 content type in a way that permits backward compatibility.

9.11.4.3 Options for MHS

Definition of interoperability parameters (see Appendix A) for use of MHS will require agreement on a number of options. The choice of such options can lead to multiple profiles. Example options are the following, in which there are suboptions defined by choice of X (interpersonal messaging user agent or electronic data interchange user agent, each with or without the requirement for a secure agent); Y (basic message store or secure message store); and G (an ADMD gateway capability is or is not required) [Ref. IGOSS 1993]:

• 1988 relay MTA [G]
• 1988 end system in which the MTA is collocated with a 1988 interpersonal message UA, an electronic data interchange UA, or both [X, G]
• An end system in which an MS and a UA are collocated with the MTA [X, Y, G]
• An end system in which an MS is collocated with the MTA [Y]
• A remote UA that is collocated with an MS [X, Y]

- A remote UA that does not require MS services [X]
- A remote UA that does require MS services [X]
- A remote MS, which serves a remote UA [Y].

A number of security classes may be defined for the Message Transfer System (MTS). These may include implementing all security mechanisms outside the MTS (e.g., within the UA or MS); implementing most security mechanisms outside the MTS but providing in the MTS services related to secure access management; and providing authentication and non-repudiation within the MTS. Each of the above example classes could be required to support end-to-end confidentiality, thus defining suboptions. [Ref. IGOSS 1993]

9.11.4.4 Profiles and for MHS

The following shows the current status of MHS ISPs:

- DISP 10611-1, *ISPs AMH1n - Message Handling Systems - Common Messaging,* Part 1: *Service Support,* 1993
- DISP 10611-2, *ISPs AMH1n - Message Handling Systems - Common Messaging,* Part 2: *Specification of ROSE, RTSE, ACSE, Presentation, and Session for Use by MHS,* 1993
- DISP 10611-3, *ISPs AMH1n - Message Handling Systems - Common Messaging,* Part 3: *AMH11: Message Transfer (P1),* 1993
- DISP 10611-4, *ISPs AMH1n - Message Handling Systems - Common Messaging,* Part 4: *AMH12: MTS Access (P2),* 1993
- DISP 10611-5, *ISPs AMH1n - Message Handling Systems - Common Messaging,* Part 5: *AMH13: MS Access (P7),* 1993
- DISP 11189, *ISP FDI2 - MHS Use of Directory,* 1993.

DISP 11189 specifies that the following functions be used to access Directory services for UAs [Ref. IGOSS 1993]:

- Verify the existence of a Directory Name
- Return the originator/recipient address(es) that correspond to a Directory Name
- Determine whether a Directory Name presented denotes a user or a Distribution List
- Return the members of a Distribution List
- Return the capabilities of the entity referred to by a Directory Name (e.g., in support of a particular body part)
- Return the public key or certificate referred to by a Directory Name.

9.11.4.5 Common MHS Message Format for NATO (ACP 123)

Overview. Beginning in May 1990, subject matter experts from many nations met to develop a common messaging strategy that can be deployed to facilitate interoperability among the Allies. The strategy, which will include the definition of a new Common Message Format (CMF) and corresponding procedures, is to be based on X.400. The end goal is to replace the existing messaging system currently based on the Allied Communications Publication 127 (ACP 127) and associated documentation (i.e., ACP 117 and ACP 121). (ACPs are meant for use in NATO and other nations such as Australia and New Zealand.) The X.400-based ACP will be called ACP 123. Major work has been completed in the area of requirements, and some, but not all, procedural issues have been resolved. The new standard will satisfy not only the ACP 127 requirements, but also national requirements such as the US Joint Army, Navy, Air Force Publication (JANAP) 128 message requirements. The work will use the MMHS work of the

TSGCE SG9, including the mappings between ACP 127 and X.400 that have been defined in draft STANAG 4406 (see Section 17.3.4.2). [Ref. ACP 123 1991]

ACP 127. Allied Communications Publication (ACP 127) is a message formatting standard commonly used by Allied nations. Derivatives of it—ACP 126 and Joint Army, Navy, Air Force Publication (JANAP) 128 are also in common use. ACP 117 and ACP 121 are associated procedural documents. ACP 123 was selected as the designation for the new X.400-based military messaging system.

AMH-ISME. Allied Message Handling (AMH) International Subject Matter Expert (ISME) meetings were conducted in May 1990 and March 1991 with the following goals:

- Develop a common messaging strategy that can be deployed to facilitate interoperability among the Allies
- Include definitions of common message formats (CMFs) and corresponding sets of procedures based on X.400-1988
- Replace the existing messaging systems currently based on ACP 127 and its associated documents (ACP 117 and ACP 121).

ACP 123 Task Force. The US DoD Defense Communications Agency (now DISA) initiated in July 1990 an ACP 123 Task Force to become the focal point for developing the X.400-based ACP 123 for the United States. One product of this group was the ACP Requirements Document [Ref. ACP 123 1991], which specifies the ACP 127 and JANAP 128 message requirements on a line-by-line basis and provides recommendations on how those requirements might be implemented using existing or newly defined X.400 services. Their work is being conducted under the auspices of the Defense Message System (DMS).

Modern Message Handling. A Modern Message Handling working group met in October 1991 and January 1992 to address ACP 123 requirements. Initial meetings of this working group were held at NACISA. SHAPE supported this working group in 1991 and 1992, but SHAPE support for ACP 123 ended in 1992 when the reorganization (downsizing) of SHAPE beginning in January 1993 did not contain tasking on ACP 123. [Ref. Lawn 1994]

Content of ACP 123. ACP 123 has three chapters and several annexes. The annexes address ASN.1 definitions and object identifiers. The three chapters address the following:

(1) Introduction and definition of terms and abbreviations

(2) Common elements of service, X.400 elements of service, and military extensions

(3) MHS components (e.g., MTS, UA, MS); procedures; security; naming and addressing; and management.

9.11.5 Manufacturing Message Specification (MMS)

9.11.5.1 MMS Standards and Relation to MAP

A Manufacturing Message Specification (MMS) has been defined to provide for client-server[49] message-based communications between programmable devices in a computer-controlled environment [Ref. IGOSS 1993]. MMS is the key component of the Manufacturing Automation Protocol (MAP), the OSI protocol promoted worldwide by General Motors, now in Version 3.0.[50]

---

[49] The client-server roles are MMS-service specific. The client is the system that exercises control, and the server is the system being controlled. A device may provide support services of client, server, or both.

[50] MAP is associated with another standard, Technical Office Protocol (TOP) (see Section 15.1.3.6).

MMS was originally developed as Electrical Institute of America (EIA) RS-511 [Ref. INI 1987]. The MMS standard has four parts:

- ISO 9506-1, *Manufacturing Message Specification*, Part 1: *Service Definition*
  - AM 1: *Data Exchange*, 1993
- ISO 9506-2, *Manufacturing Message Specification*, Part 2: *Protocol Specification*
  - AM 1: *Data Exchange*, 1993
- ISO 9506-3, *Manufacturing Message Specification*, Part 3: *Companion Standard for Robotics*
- ISO 9506-4, *Manufacturing Message Specification*, Part 4: *Companion Standard for Numerical Control*

The MMS standard defines 86 different messaging services. Example (all required in IGOSS) are initiate, conclude, abort, reject, and identify. Both IGOSS and MAP 3.0 (see Section 15.1.3.6) define implementation classes of services, in which Class 0 comprises the five services identified above. While MMS is a standard primarily used for industrial automation, it is included because its wide use may affect some military message standards. Section 9.13.6 discusses the time-critical communications requirements of MAP.

The MMS work in ISO is under TC184/SC5/WG1, which is responsible for communications systems in the area of industrial automation. [Ref. Kirk 1990] In 1989, a new work item to develop an international standard, *Framework for CIM Systems Integration*, was assigned to SC5/WG1. Efforts are focused on ENV 40 003 based on the CIM-OSA work from the European Strategic Programme of Research and Development in Information Technology (ESPRIT). MMS is included in IGOSS (see Section 16.1.3.3).

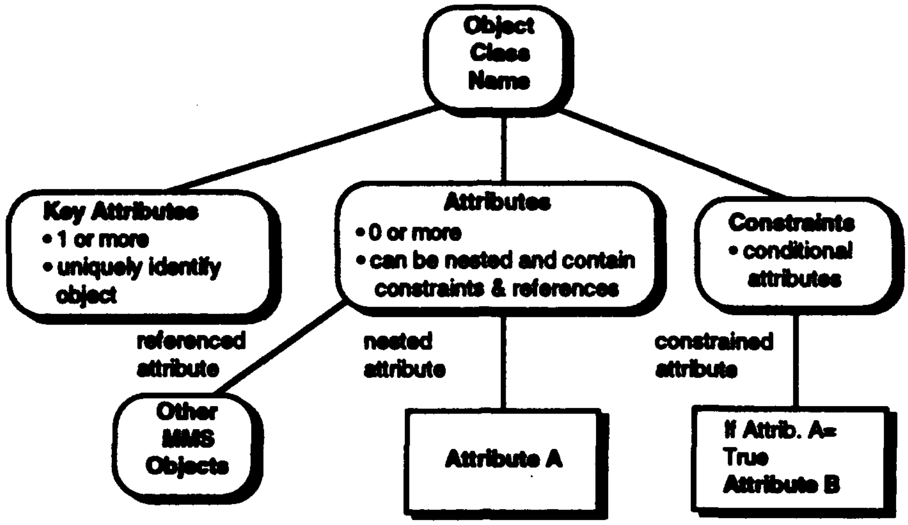
9.11.5.2 MMS Overview[51]

MMS uses object oriented methodology to model the items and entities required for communication among manufacturing devices. MMS services operate on MMS objects. An object model is specified for the various components of an MMS environment: Virtual Manufacturing Devices (VMDs), domains within VMDs, program invocations within VMDs, variables and data within VMDs, and several others. MMS objects are built from attributes and constraints (Figure 13).

MMS uses the client/server approach to distribute services across devices on the network. Typically, the client is a host computer and the server is some factory floor device.

MMS is unique among the OSI application standards due to companion standards. Companion standards allow MMS to provide additional detail focused on a particular type of factory floor device. The companion standard mechanisms are inherent throughout the base MMS specification. For example, 53 of the 86 MMS services are specifically designed for extension. Additionally, 8 of the 18 MMS objects are specifically designed for extension. For example, the MMS companion standard for robots provides a description of a robot arm object. This description then becomes an extension of the base VMD object. A companion standard can add to the base MMS specification the following items: specification of extra parameters in the service primitives, specification for additional detail attributes in MMS object definitions, and additions to the protocol procedures and the protocol behavior.

[51] This section has been excerpted from [Tang 1991].



Source: [Tang 1992].

Figure 13. Structure of Objects for MMS

9.11.6 File Transfer, Access, and Management (FTAM)

Both FTAM and MHS (ITU-TS X.400) (see Section 9.11.4) can be used for carrying many forms of messages. Where an X.400 MHS is already in place and the destinations may not always be on line, X.400 (1988) with a message store may be the best option. Where there is a requirement for heavy traffic or immediate transfer and acknowledgment, FTAM may be the better solution. [Ref. OSN 1992a]

NIST Special Publication 500-196, *Guidelines for the Evaluation of File Transfer, Access and Management Implementations* helps users acquire FTAM implementations [Ref. CSL 1992, p.2] just as NIST SP 500-182 does for MHS implementations (see Section 9.11.4).

9.11.6.1 FTAM Overview[52]

File handling is one of the principal services in a networking environment. Many existing file protocols are concerned primarily with moving complete files. The File Transfer Access Management (FTAM) standard, which is specified in ISO/IEC 8571, has broadened the scope of these protocols by offering three modes of file manipulation: file transfer, file access, and file/filestore management. File transfer is the movement of a complete file between two filestores in different open systems. File access performs reading, writing, or deleting of selected parts of a remote file. File/filestore management refers to the management of a remote file/filestore.

Organization of a file is operating-system specific—a file may be considered a sequence of bytes in one system and a series of records in another. In order to accommodate heterogeneous file systems, the FTAM standard introduces the concepts of a virtual file and a virtual filestore. Virtual files and virtual filestores are the OSI abstractions of real files and real filestores. The use of virtual files and virtual filestores permits applications to perform file operations over a variety of file types without detailed knowledge of the characteristics of the remote file systems. Since virtual filestores and virtual files are only abstractions, an FTAM implementation needs to provide translation between virtual files and system-specific files.

---

52 Portions of this section have been excerpted from [Tang 1991].

FTAM is an asymmetric protocol involving two objects: an initiator and a responder. An initiator initiates an application association with a responder for its subsequent file activities, while a responder maintains a virtual filestore containing virtual files that are the subjects of file activities by different initiators. The initiator is normally invoked by a local user's request and supplied with information about a local file and a remote virtual file. The responder is informed of the file operations through the PDUs exchanged with the initiator.

The term FTAM dialogue is used to qualify the application association between an initiator and a responder. It is possible that the same responder maintains more than one FTAM dialogue, or the same initiator maintains more than one FTAM dialogue. An initiator or a responder identifies a role of an application entity for an FTAM dialogue. The same entity can simultaneously play different roles for different FTAM dialogues.

9.11.6.2 FTAM Standards

FTAM defines a file service and specifies a file protocol within the Application Layer (Layer 7). The standard is concerned with identifiable bodies of information that can be treated as files, which may be stored within open systems or passed between application processes. ISO 8571 defines the basic file service for FTAM. It provides sufficient facilities to support file transfer and establishes a framework for file access and file management. This standard does not specify the interfaces to a file transfer or access facility within the local system. An addendum may be added that reflects quality of service developments and integration. The FTAM standard currently has five parts with amendments and addenda. Addendum 1 (Filestore Management) defines a hierarchical file system with subdirectories, links, paths, etc. An additional standard describes a performance test suite. Second editions to the FTAM standard (Parts 1-5) are underway. The pertinent FTAM standards are:

- ISO 8571-1 (Part 1): *General Introduction*, 1988
  - AM 1, *Filestore Management*, December 1992
  - AM 2, *Overlapped Access*, August 1993
  - AM 3, *Service Enhancement*, December 1993
  - WDAM 4, *Security Enhancement* (project suspended July 1993)
  - WD 8571-1 (Part 1): *General Introduction*, Edition 2 (incorporates AM 1), 1992
- ISO 8571-2 (Part 2): *Virtual Filestore Definition*
  - AM 1, *Filestore Management*, December 1992
  - AM 2, *Overlapped Access*, August 1993
  - PDAM 3, *Enhancement for FTAM Services to Satisfy Additional User Requirements* (project suspended as 1993 PDAM has null content)
  - WDAM 4, *Security Enhancement* (project suspended July 1993)
  - WD 8571-2 (Part 2): *Virtual Filestore Definition*, Edition 2 (incorporates AM 1), 1992
- ISO 8571-3 (Part 3): *File Service Definition*
  - AM 1, *Filestore Management*, December 1992
  - AM 2, *Overlapped Access*, August 1993
  - AM 3, *Service Enhancement*, December 1993
  - WDAM 4, *Enhancement to FTAM Security Services* (project suspended July 1993)
  - WD 8571-3 (Part 3): *File Service Definition*, Edition 2 (incorporates AM 1), 1992

- ISO 8571-4 (Part 4): *File Protocol Specification*
  - AM 1, *Filestore Management*, December 1992
  - AM 2, *Overlapped Access*, August 1993
  - AM 3, *Service Enhancement*, December 1993
  - AM 4, *Defect Report Changes*, November 1992
  - WDAM 5, *Enhanced Security for FTAM* (project suspended July 1993)
  - WD 8571-4 (Part 4): *File Protocol Specification*, Edition 2 (incorporates AM 1), 1992
- ISO 8571-5 (Part 5): *PICS Proforma*, December 1990
  - PDAM 1, *Filestore Management*, July 1992 (editing meeting January 1994)
  - WDAM 2, *Overlapped Access* (in the absence of a new WD, SC21 proposed in July 1993 to reassess this project)
  - WDAM 3, *Enhancement to FTAM Services to Satisfy Additional User Requirements* (to be progressed as a technical corrigendum)
  - WDAM 4, *Enhancement to FTAM Security Services* (project suspended July 1993)
  - WD 8571-5 (Part 5): *Protocol Implementation Conformance Statement Proforma*, Edition 2 (rapporteur meeting January 1994)
- *Conformance Test Suite for the FTAM Protocol* has the following parts:
  - ISO/IEC 10170-1 (Part 1): *Test Suite Structure and Test Purposes*, January 1993 [SC21 N 7530]
  - WD 10170-2 (Part 2): *FTAM Abstract Test Suite* (CD expected October 1994; however, this project risks cancellation by SC21 in the absence of written confirmation that the regional workshops will provide a WD by June 1994. [Ref. SC21 N 7728 1993])
  - WD 10170-3 (Part 3): *ACSE Abstract Test Suite Embedded Under FTAM* (CD expected October 1994)
  - WD 10170-4 (Part 4): *Presentation Abstract Test Suite Embedded Under FTAM* (CD expected October 1994)
  - WD 10170-5 (Part 5): *Session Abstract Test Suite Embedded Under FTAM* (CD expected October 1994).

The current FTAM standard treats a filestore as an unstructured collection of files. Amendment 1 defines a structured filestore to allow the organization and manipulation of individual groups of files. Amendment 2 on Overlapped Access allows more efficient access to contents of a structured file. The Overlapped Access draft specification uses the formal description language LOTOS. These extensions will support needs of the Network File Store, but harmonization with Document Transfer and Manipulation (DTAM) (ITU-TS) and Document Filing and Retrieval (DFR) (SC18) will be needed. PICS proformas such as ISO 8571-5 provide a framework for specifying compliance with all the interoperability parameters for the implementation of a protocol; this concept is discussed in Section 12.2.2.

In order to cope with the wide range of possible file mechanisms, FTAM uses a virtual filestore model. In FTAM's virtual filestore model, files are structured. Each file has a set of attributes (e.g., owner information and contents type), in addition to the data association with the file. The contents type of the file defines the file structure. Currently FTAM is not easily exportable to other application services. The new work will attempt to improve efficiency by reducing the number of confirmed requests (e.g., needed for file transfer over long-haul communications); extending and simplifying FTAM services to allow other applications services (e.g., TP) to easily use FTAM providing services (e.g., for data transfer) with minimum overhead

by providing high-level services; and providing file services for other user services, such as ITU-TS telematic services.

WG5, reporting on the status of ISO 8571-2/DAM 3 in May 1992, raised the following issues:

- An international Registration Authority for Objects does not yet exist
- Additional document types are under development that may need to be incorporated in 8571-2 as part of this project
- Additional generalized constraint sets (file structure) are under development that may need to be incorporated in 8571-2 as part of this project.

As these issues have yet to be resolved, WG5 believes that the project is still active. [Ref. SC21 N 7162 1992]

As a consequence of the proliferation of FTAM implementations over the past few years, the document types included in the base standard are not sufficient for the wide variety of applications served by FTAM. For example, new document types for CGM, EDI, and COBOL have been submitted to the FTAM Group for comment and review. The FTAM group believes that ISO should set up an International Document Type Registry where the already defined document types can be held and publicized. Moreover, ISO should set up a mechanism to manage the document types that involve those ISO Groups. [Ref. SC21 N 6229 1991]

In addition, some existing document types include optional facilities that have led to interoperability problems. It was therefore proposed in June 1991 that document type definitions include a statement of conformance requirements. This information could be included as Annex F to ISO 8571-2 or as a Tutorial Addendum on Interoperability in ISO 8571. [Ref. SC21 N 6230 1991]

SC21/WG5 is developing a document type to enable FTAM to transfer CGM files as a structured file rather than (with current FTAM) as a transparent sequence of octets. The new work would provide access to the whole metafile, to the metafile descriptor, or to the individual pictures with an associated metafile descriptor. All three CGM encoding techniques would be supported: binary, clear text, and character text. [Ref. SC 21 N 4192 1989] The FTAM Rapporteur Group reviewed the latest version of the CGM document type in May 1991, found it technically satisfactory, and recommended that it be registered following the *Procedures for the Registration of Document Types* (ISO 9834, Part 2). [Ref. SC21 N 6225 1991]

In May 1991, SC21 WG5 proposed an EDIFACT/FTAM Document Type (see also Section 7.1.4) in an attempt to merge existing FTAM implementations with existing EDI systems with a minimum of change. [Ref. SC21 N 6224 1991] DAM 3, *Service Enhancement* to ISO 8571-2, *FTAM Virtual Filestore Definition*, includes the CGM and EDIFACT document types.

In August 1991, a new work item (NWI) on the *Definition of a New FTAM Document Type for Directory* was proposed to define an FTAM document type that represents Directory information, which would be used when FTAM is transferring Directory information. The NWI failed to qualify for acceptance to the Program of Work.

Since the rejection of this NWI for an FTAM Document Type, several new developments have occurred. The first is a NWI proposal for a *Generic ASN.1 Document Type*, which would allow an exact mapping of any ASN.1 defined body of information to be transferred by FTAM without the need of additional specification. The second is the rapid progression of the "Enhanced

Services" amendment to FTAM whose main purpose was specifically to allow FTAM to be easily utilized by other ASEs. [Ref. SC21/WG8 N 63 1992]

At the SC21 Plenary in May 1992, the UK proposed a new work item on a *Class of Mappings from a Single ASN.1 Type to an FTAM Document Type*. The proposal was for a new part of the FTAM standard to specify a generic FTAM Document Type. This type would be used to define arbitrarily many specific FTAM Document Types by supplying only an ASN.1 type definition and an ASN.1 Object Identifier to identify the resulting FTAM Document Type. The resource requirements necessary to forward this proposed NP to JTC1 for letter ballot were not met (i.e., at least five national bodies willing to actively participate). Therefore, this Proposed NP was returned to SC21. [Ref. SC21 N 7443 1992]

In March 1992, the United States noted the following problem with certifying FTAM implementations as conformant. Some OSI certification agencies will not certify FTAM implementations as conformant when the implementation, in the role of an initiator, does not employ all possible protocol variations, even though the protocols that are used completely support the services of the implementation. It follows that the appropriate standards should be clarified so as to allow the certification agencies to deselect, within permitted bounds as defined by the standard, tests that exercise protocols not used to support the claimed services of the product. Although the problem presently concerns FTAM, it may occur in products implementing other standards where there is an asymmetric relationship between correspondents and where the initiator controls the protocol that will be exchanged. [Ref. SC21 N 6802 1992]

EWOS is developing a Remote Action (RA) service and protocol for use with FTAM to support the ability to perform a remote action upon completion of a file operation. Examples of a remote action would be execution of a batch job that is transferred to another system via FTAM and to spool a print file to a printer after being transferred using FTAM. Both RPC and JTM could provide this support, but JTM is viewed in EWOS as too complex for simple remote actions. RA would not compete with JTM and specifically would not support such JTM services as gathering information for input to a job, spawning jobs to several systems, manipulating entries in job queues (e.g., kill a job), monitoring progress of jobs, or preparing progress reports. [Ref. EWOS 1990]

The FTAM standards include an annex, *Commitment Control with File Transfer*, which defines a specific example of how FTAM could be used with CCR. This was originally developed when CCR was at DIS status. In response to an earlier defect, this annex was suspended until CCR restabilized. Following the publication of CCR, an input document was drafted to replace the old annex. During the process of drafting the annex, it became apparent that while FTAM can recover from an application or communication failure during data transfer, CCR treats a failure before the end of Phase I as a (presumed) rollback. This relation between FTAM recovery and CCR recovery requires careful examination. [Ref. SC21 N 6228 1991]

9.11.6.3 Options for FTAM

Definition of interoperability parameters (see Appendix A) for use of FTAM will require agreement on a number of options. The choice of such options can lead to multiple profiles. An example is the choice of positional file transfer, management, and simple file access—all three are required in IGOSS (see Section 16.1.3.3) but not in other profiles. In addition the documents supported need to be specified in a profile.

9.11.6.4 Profiles for FTAM

The ISO FTAM standard (ISO 8571-2, Annex B) provides for three document types: unstructured text, sequential text, and unstructured binary. OIW Stable Implementor's Workshop agreements have been published by NIST for four others: sequential file, random access file, indexed file, and file directory file. Six implementation profiles have been defined by the European Standards Promotion and Application Group (SPAG), which have the following corresponding profiles from the NIST OSI Implementor's Workshops:

- *Simple File Transfer* (SPAG A/111, NIST T1, ENV 41 204)
- *Positional File Transfer* (SPAG A/112, NIST T2, ENV 41 206)
- *Full File Transfer* (SPAG A/113, NIST T3)
- *Simple File Access* (SPAG A/122, NIST A1)
- *Full File Access* (SPAG A/123, NIST A2)
- *Management* (SPAG A/13, NIST M1).

International Standardized Profiles (ISPs) are finalized by regional workshops and submitted for ISO acceptance by the JTC1 Special Group on Functional Standardization (SGFS). There are currently six parts to ISO/IEC 10607 and one part to DISP 11190 on FTAM ISPs:

- ISO/IEC ISP 10607-1, *ISPs AFT nn - File Transfer, Access, and Management,* Part 1: *Specification of ACSE, Presentation and Session Protocols for the Use by FTAM*
  - DAM 1, *Additional Specifications for COBOL Document Types*
- ISO/IEC ISP 10607-2, *ISPs AFT nn - File Transfer, Access, and Management,* Part 2: *Definition of Document Types, Constraint Sets and Syntaxes*
  - DAM 1, *Additional Definitions*
  - DAM 2, *Additional Specifications for COBOL Document Types*
  - DAM 3, *FTAM Constraint Set and Document Type for CGM*
- ISO/IEC ISP 10607-3, *ISPs AFT nn - File Transfer, Access, and Management,* Part 3: *AFT 11 - Simple File Transfer Service (Unstructured)*
- ISO/IEC ISP 10607-4, *ISPs AFT nn - File Transfer, Access, and Management,* Part 4: *AFT 12 - Positional File Transfer Service*
  - DAM 1, *Additional Specifications for COBOL Document Types*
- ISO/IEC ISP 10607-5, *ISPs AFT nn - File Transfer, Access, and Management,* Part 5: *AFT 22 - Positional File Access Service*
  - DAM 1, *Additional Specifications for COBOL Document Types*
- ISO/IEC ISP 10607-6, *ISPs AFT nn - File Transfer, Access, and Management,* Part 6: *AFT 12 - File Management Service*
- DISP 11190, ISP FDI3 - *FTAM Use of Directory*, 1993.

9.11.7 Directory

ITU-TS is developing a database application standard for logically storing directory information. The Directory is a distributed database on users, processes, and other objects, used to provide access to information that people or processes require prior to communicating. The standards are in the following X.500 Series recommendations: X.500, X.501, X.509, X.511, X.518, X.519, X.520, and X.521. A report by Ovum, *X.500 and the Electronic Directory: the Business Opportunity*, predicts that the Directory market will grow to $574 million in the year 2000. [Ref. OSN 1992b]

9.11.7.1 Directory Services and Models[53]

Directory Services. The Directory services provide a specialized hierarchical database for OSI applications. The Directory contains information about objects and provides structured mechanisms for accessing that information. These services are intended to provide user friendly naming to permit a user to specify an object's name and then retrieve additional addressing information. The two key aspects of the OSI Directory, which distinguish it from other database and name-server work, are [Ref. OSN 1990d]:

- The Directory can be read, modified, and searched remotely via OSI protocols.
- A highly distributed database is provided by Directory System Agents (DSAs).

Directory Models. The following four models define the Directory services [Ref. OSN 1990d]:

- The informational model describes the Directory Information Base (DIB). The DIB contains all the information to which the Directory provides access. This model is concerned only with the logical structuring of the information.
- The functional model describes interactions that take place between the various DSAs that comprise the Dictionary.
- The organizational model describes how portions of the Directory tree map onto the DSAs. This includes issues of replication and access control.
- The security model of Directory services describes the service in terms of authentication and authorization.

The DIB model is a conceptual information model storing information about OSI objects. It is structured hierarchically using a tree structure known as the Directory Information Tree (DIT). The Directory standard provides Directory schema that can be used by a profile group to define its DIT.

Directory Entries. The DIB comprises object entries and alias entries. An object entry is the primary collection of information in the DIB about an object in the real world. An alias entry points to another object entry and is primarily used to provide a user-friendly name to the referenced object entry. An object in the real world can be represented by more than one alias although it can be represented by at most one object entry in the DIB.

Directory Attributes. An entry is described by a set of attributes. Table 26 shows some of the attribute types defined by the Directory standard. Attribute types can also be defined by profile groups. Among the attributes of an entry, there are the distinguished attributes that are used to name the entry. The type used in a distinguished attribute is called a distinguished attribute type, while some of the attribute values (normally at most one) of a distinguished attribute type are called distinguished values.

Directory Classes. Entries of similar characteristics are grouped into object classes. Examples of object classes are Country, Organization, Person, Alias, Application Entity, DSA, and Device. A specification of an object class describes (mandatory) attributes that must belong to the Person object class by requiring the Common Name and Surname attributes to be mandatory, and the Telephone Number and User Password attributes to be optional.

Directory Structure. The structure of the DIB is described by the Directory schema. The Directory schema consists of a set of structural rules on the DIT. It provides templates for the definition of object classes, attribute types, and abstract syntaxes. Object classes, attribute types,

---

53 Portions of this section have been excerpted from [Tang 1991].

and attribute syntaxes are defined by a profile group or a Directory administrator. The Directory schema, in providing templates for these definitions, can improve consistency in the definitions. For instance, it prevents the creation of an inappropriate containment relation in the DIT, the use of an inappropriate attribute type in an object class definition, and the addition of an inappropriate value of a syntax not matching the syntax defined for the attribute type.

Table 26. Directory Attribute Types

X.500 Attribute Types			
System	Object Class Aliased Object Name Knowledge Information	Labeling	Common Name Surname Serial Number
Geographical	Country Name Locality State or Province Street Address	Organizational	Organization Organization Unit Title
Explanatory	Description Search Guide Business Category	Postal	Postal Address Postal Code Post Office Box Physical Delivery Office
Telecommunications	Telephone Number Telex Number Telex Terminal ID Fax Telephone Number International ISDN Number Registered Address Destination Indicator	Preferences	Preferred Delivery Meth
		OSI Application	Presentation Address Supp. Application Context
		Security	User Password User Certificate CA Certificate
Relational	Member Owner Role Occupant		Authority Revocation List Certificate Revocation List Cross Certificate Pair

Source: [Tang 1992].

Directory Distributed Services. In a large network environment, the Directory services may be distributed among multiple DSAs. Despite the distributed nature, the basic philosophy of the Directory services is transparent distribution (i.e., a DUA views the Directory as a single object). This means that the object entry information retrieved by a DUA from a particular DSA should be the same, had the object entry information been retrieved from a different DSA. To preserve the DUA's view of a single Directory object, mechanisms must be defined to allow partitioning of the DIB.

One of the design goals of the Directory services is that requests addressed to any DSA must produce results that are the same regardless of the DSA contacted. To satisfy this goal, a DSA must have some knowledge of the place where the requested information is located in the DIT. In the extreme case, the entire DIB is contained within a single DSA, in which case the goal is trivially satisfied. In fact, a centralized DSA was very common during the early DSA implementations. In general, information in the DIB is distributed among the DSAs. Each DSA maintains one or more substructures of the DIT. Consequently, the DSAs may need to communicate with each other to resolve requests from a DUA.

Directory Protocols. When a DUA conveys a request to a DSA and a DSA responds, the Directory Access Protocol (DAP) is used. If the DSA contacted by the DUA cannot process the request, it may propagate or "chain" the request to another DSA that may repeat the chaining operation, or the initial DSA may provide the DUA with a "referral" to another DSA more likely to contain the information. The protocol used among DSAs to convey a service request is known as

the Directory System Protocol (DSP). When DSAs replicate information to enhance availability and performance, two other protocols are used. The Directory Operational Binding Management Protocol (DOP) is used to initialize or terminate a relationship between two DSAs regarding the supply and consumption of replicated information and knowledge regarding the content of DSAs. The Directory Information Shadowing Protocol (DISP) is used to initially provide and refresh replicated information. [IGOSS 1993].

9.11.7.2 Directory Standards

SC21/WG4 and ITU-TS are working on OSI directories. Second editions to Parts 1-8 of *The Directory* (ISO 9594) are expected by the end of 1994 (the ITU-TS ballot closed November 1993). The status of standards for the Directory are as follows:

- ISO/IEC 9594-1, *The Directory*, Part 1: *Overview of Concepts, Models and Services*, December 1990 (X.500)
  - AM 1, *Replication, Schema and Access Control*
  - WD 9594-1/9 WDAMs, Amendments to Parts 1 to 9 on *Internationalization of the Directory Enhancement of Directory*, June 1993 [SC21 N 7931] (PDAMs expected July 1994)
  - WD 9594-1/9 WDAMs, Amendments to Parts 1 to 9 on *Enhancement of Directory Operational Security*, June 1993 [SC21 N 7932] (PDAMs expected November 1994)
  - WD 9594-1/9 WDAMs, Amendments to Parts 1 to 9 on *Directory Schema Migration*, June 1993 (new work item proposal) [SC21 N 7942] (PDAMs expected November 1994)
  - DIS 9594-1.2, *The Directory*, Part 1: *Overview of Concepts, Models and Services*, Edition 2 (incorporates AM 1), 1993 (X.500:1993)
- ISO/IEC 9594-2, *The Directory*, Part 2: *Models*, December 1990 (X.501)
  - AM 1, *Access Control*
  - AM 2, *Schema Extensions*
  - AM 3, *Replication*
  - DIS 9594-2.2, *The Directory*, Part 2: *Models*, Edition 2 (incorporates AM 1, AM 2, and AM 3), 1993 (X.501) (X.501:1993)
- ISO/IEC 9594-3, *The Directory*, Part 3: *Abstract Service Definition*, December 1990 (X.511)
  - AM 1, *Access Control*
  - AM 2, *Replication, Schema and Enhanced Search*
  - ISO 9594-3.2, *The Directory*, Part 3: *Abstract Service Definition*, Edition 2 (incorporates AM 1 and AM 2), 1993 (X.511:1993)
- ISO/IEC 9594-4, *The Directory*, Part 4: *Procedures for Distributed Operations*, December 1990 (X.518)
  - AM 1, *Access Control*
  - AM 2, *Replication, Schema and Enhanced Search*
  - ISO 9594-4.2, *The Directory*, Part 4: *Procedures for Distributed Operations*, Edition 2 (incorporates AM 1 and AM 2), 1993 (X.518:1993)
- ISO/IEC 9594-5, *The Directory*, Part 5: *Protocol Specifications*, December 1990 (X.519)
  - AM 1, *Replication*
  - ISO 9594-5.2, *The Directory*, Part 5: *Protocol Specifications*, Edition 2 (incorporates AM 1), 1993 (X.519:1993)

- ISO/IEC 9594-6, *The Directory*, Part 6: *Selected Attribute Types*, December 1990 (X.520)
  - AM 1, *Schema Extensions*
  - ISO 9594-6.2, *The Directory*, Part 6: *Selected Attribute Types*, Edition 2 (incorporates AM 1), 1993 (X.520:1993)
- ISO/IEC 9594-7, *The Directory*, Part 7: *Selected Object Classes*, December 1990 (X.521)
  - AM 1, *Schema Extensions*
  - ISO 9594-7.2, *The Directory*, Part 7: *Selected Object Classes*, Edition 2 (incorporates AM 1), 1993 (X.521:1993)
- ISO/IEC 9594-8, *The Directory*, Part 8: *Authentication Framework*, December 1990 (X.509:1988)
  - AM 1, *Access Control*
  - WDAM, *Extensions for Certificate Identifications*, 1993 (new work item accepted April 1993; PDAM expected July 1995)
  - DIS 9594-8.2, *The Directory*, Part 8: *Authentication Framework*, Edition 2 (incorporates AM 1), 1993 (X.509:1993)
- ISO 9594-9, *The Directory*, Part 9: *Replication*, November 1993 (X.525:1993).

The following standards are under development by ISO:

- WD 9594-10, *PICS Proforma, for the OSI Directory DUA Protocol*, December 1990 (fast track ballot of ITU-TS standard has been requested) (X.581:1992)
- WD 9594-11, *PICS Proforma, for the OSI Directory DSA Protocol*, December 1990 (fast track ballot of ITU-TS standard has been requested) (X.582:1992)
- WD 9594-w, *Use of Systems Management for Administration of the Directory*, June 1993 [SC21 N 7930] (CD expected in July 1994, DIS in July 1995, and IS in July 1996).

The scope of WD 9594-w is to define a set of Managed Objects to support Directory operational information (i.e., that information the Directory uses to guide its own operations). Requirements for management of Directory systems (e.g., performance, accounting) need to be determined as well as consideration and identification of the most appropriate mechanisms and protocols to be used to provide the various administration services for the Directory. This operational information would be accessible through the CMIS and CMIP; however, the Directory Information Base will continue to be only accessible through the Directory Services and Protocols.

The ITU-TS Directory Defect Resolution Committee has produced a *Directory Implementor's Guide*, January 1993 [SC21 N 7566], which is a compilation of reported defects in the 1988 ITU-TS X.500 Recommendations (ISO/IEC 9594) standards and their resolutions. It is a ITU-TS record of defects, not a formal ISO record of Directory defects, intended to be an authoritative source of information for implementors to read in conjunction with the Recommendations/Standards themselves. [Ref. SC21 N 6012 1991] The Guide provides guidance to implementors on how they may submit defects as well as insights into the procedures by which their reported defects will be processed.

In a liaison statement to SC6 concerning a request for incorporation of new protocol information attributes in 9594-6/AM 1, SC21 states that it would be an error to introduce networking information into the OSI (Application) Directory. Instead, SC21 believes these requirements should be satisfied in Network directory facilities. [Ref. SC21 N 6974 1992]

9.11.7.3 Enhancements to Directory Standards

Although the Directory has introduced a type for strings encoded in the Universal Coded Character Set (UCS) (ISO 10646), the UK has argued that it is insufficient for the Directory to support an international, distributed environment. Instead, a fully international Directory must address (1) local users using a local writing system and character set and (2) external users who use different writing systems and character sets. The UK, therefore proposed that work should be started to cover the following [Ref. SC21 N 6821 1992]:

- Locale-dependent operations involving string handling
- Alternative names as Relative Distinguished Names (RDN)
- Locale-dependent alternate attribute values.

In June 1992, SC21 accepted a proposal for a NWI entitled *Internationalization of the Directory* [SC21 N 7019 1992], which it assigned to WG4 for development. [Ref. SC21 N 7579 1993] The NP will result in an addendum or addenda to ISO 9594-1 and ISO 9594-9. It is in WD status [SC21 N 7931, June 1993] and the target dates are PDAM in May 1994, DAM in May 1995, and AM in May 1996.

JTC1 has accepted a NWI for Certificate Definitions [SC21 N 7102]. The NWI would be an amendment to ISO 9594-8 and would extend the definitions of the Certificate Revocation List, User Certificate, and Revocation Certificate. This work should not be confused with another NP [SC21 N 7020] (see Section 11.2.2.7) that will address the use of 9594-8 Certificates to provide authentication and some other related security services.

The Directory group, at its May 1992 meeting decided that the Directory standard would have to be extended to use the Upper Layer Security services. Thus, they are submitting a proposal for an NP [SC21 N 7020] on enhancement of directory operational security (see also Section 11.2.2.7). [Ref. SC21 WG4 N 1527 1992]

9.11.7.4 Example Interoperability Parameters for Directory

Two international groups are working on functional standards (profiles) for the Directory. The issues being addressed by the OIW Directory Services SIG and the EWOS/ETSI Directory Expert Group indicate options within the Directory standard and areas where baseline standards may be exceeded to address practical implementation problems. Examples of the issues and options are [Ref. IST/21: 1868 1989]:

- Classification of minimum schema capabilities.
- Classification of baseline structure rules—mandates the capability to access a standard Directory tree (which may be extended to a wide variety of entries).
- Definition of maximum APDU size—eases design of high-performance DSAs (e.g., to ensure the Directory can respond in seconds) and eases network problems in providing quality of service.
- Pragmatic constraints on filters—protects the Directory from pathological conditions and potentially simplifies design.
- Holes in distributed operation definitions—there are many undefined aspects for distributed operations (e.g., how to handle errors).
- Constraints on alphabets—Directory uses T.61 strings. Directory profiles are addressing rejection of strings that contain non-T.61 characters and restrictions on permissible characters (e.g., escape characters).
- Constraints on integer values—defines a minimum size integer that must be supported.

- Classification of authentication—mandate use of simple uncorroborated authentication that supports external authentication within a closed domain.
- Augmentation of attribute syntax rules—augments the standards material with practical rules.
- ASN.1 rules—mandates support of ASN.1 identifier tags that are three octets in length (and no longer) and requires constructed string elements not to be nested more than one deep.
- Strong authentication algorithms—proposing alternatives to the use of RSA™ (a licensed product) for digital signatures.

A number of options can be defined for services provided by DUAs. Classes of these options include supported abstract operations; supported types and levels of authentication; and ability to use a Continuation Reference to progress an operation. Options for abstract operations include read, compare, list, search, add entry, remove entry, modify entry, modify Directory Name, and abandon; these may be bundled in many ways in various profiles. Two types of authentication are defined in Directory (i.e., user authentication and peer-entity authentication) and three levels of security at which authentication may be performed:

- Identify-only authentication, providing no confidence that the identity presented to the Directory is authentic
- Simple authentication, based on passwords, which may (depending on how the passwords are administered and protected) provide more confidence than identify-only authentication
- Strong authentication, based on the use of digital signatures that rely on the use of public key cryptographic techniques.

Finally, there are direction options for strong authentication. Peer-entity strong authentication may be one way (in which one peer authenticates the identity of the other peer; two way (in which both peers authenticate each other); or three way. [Ref. IGOSS 1993]

Another set of Directory interoperability parameters is defined by the options for DUAs. The two groups of DSA options are DSA category (solitary and cooperative) and the supported types and levels of authentication. A "solitary" DSA is a DSA designed to support a centralized DIT only and is unable to communicate with any other DSA, whereas a cooperative DSA is used to specify a bundle of functionality that allows a DSA to be part of a community of DSA that communicates in various ways to support a distributed DIT. A solitary DSA does not support DSP, DISP, DOP, referrals, and knowledge references. A cooperative DSA is able to cooperate, either directly or indirectly, with other DSAs to provide Directory services that are, to a large extent, independent of how the DIT is distributed. In direct cooperation, the DSP may be both a responder and an initiator, supporting the chained mode of operation. Indirect cooperation occurs when a DSA supports DAP only or when the responder role for DSP is supported. Authentication options for DSAs are similar to those for DUAs described above. [Ref. IGOSS 1993]

9.11.7.5 Standardized Profiles for Directory

The Directory ISPs under development by EWOS include:

- DISP 10615-1, *ISPs ADI nn -- OSI Directory*, Part 1: ADI 11, *DUA Support of Directory Access*, January 1993
- DISP 10615-2, *ISPs ADI nn -- OSI Directory*, Part 2: ADI 12, *DSA Support of Directory Access*, January 1993
- DISP 10615-3, *ISPs ADI nn -- OSI Directory*, Part 3: ADI 21, *DSA Responder Role*, July 1993

- DISP 10615-4, *ISPs ADI nn -- OSI Directory*, Part 4: ADI 22, *DSA Initiator Role*, July 1993
- pDISP 10615-5, *ISPs ADI nn -- OSI Directory*, Part 5: ADI 31, *DUA Support of Distributed Operations*, 1993
- pDISP 10615-6, *ISPs ADI nn -- OSI Directory*, Part 6: ADI 32, *DSA Support of Distributed Operations*, 1993
- pDISP 10615-7, *ISPs ADI nn -- OSI Directory*, Part 7: ADI 41, *Strong Authentication*, 1993
- pDISP 10616, *ISP FDI 11 - Directory Data Definitions - Common Directory Use*, September 1993
- DISP 11189, *ISP FDI2 - MHS Use of Directory*, 1993
- DISP 11190, *ISP FDI3 - FTAM Use of Directory*, 1993.

Future profiles for Directory are expected to follow the taxonomy of Table 27.

Table 27. Taxonomy for Directory Profiles

ADI 1	Directory Access Profiles (DAPs)	
	ADI 11	DUA Support for Directory Access
	ADI 12	DSA Support for Directory Access
ADI 2	Directory System Profiles (DSPs)	
	ADI 21	Responder Role
	ADI 22	Initiator Role
ADI 3	Distributed Operations Profiles	
	ADI 31	DUA Support of Distributed Operations
	ADI 32	DSA Support of Distributed Operations
ADI 4	Security Profiles (e.g., strong use of authentication)	
ADI 5	Shadowing and Replication Profiles	
ADI 6	Directory Administration Profiles	
	ADI 61	Administrative Area Definition and Granularity
	ADI 62	Collective Attributes
	ADI 63	Schema Administration
	ADI 64	Operational Behavior
	ADI 65	Knowledge Administration
FDI 1	Directory Data Definition (Schema Profiles)	
	FDI 11	Common Directory Use
	FDI 12	Collective Attributes
	FDI 13	Schema Management
	FDI 14	DSA Model Information
	FDI 15	Operational Attributes
FDI 2	MHS Use of Directory	
FDI 3	FTAM Use of Directory	
FDI 4	EDI Use of Directory	
FDI 5	TP Use of Directory	

Sources: WDTR 10000-2.4 , August 1993 and [EWOS/TA/93/424 1993], October 1993.

9.11.8 Job Transfer and Manipulation (JTM)

JTM (ISO/IEC 8831 and 8832) was originally designed for remote off-line (batch) processing. It uses a processing model based on movement of entities called "documents" and the exchange of these entities with users. Exchanges are specified in work specifications that include a data structure and an envelope carrying the document. In Basic Class JTM a single document can be sent to a processing element. In Full JTM (ISO 8832/AM1, *Full Class Protocol)* multiple documents and multiple processing steps are permitted. Capabilities of JTM are being included in standards for FTAM (e.g., RA) and the ASEs (e.g., RPC). [Ref. SC21 N 4356 1990]

The United States stated in ISO in March 1990 that there are no US user requirements nor any organization in the United States willing to provide resources for JTM standards. [Ref. SC21 N 4641 1990] AFNOR has similarly found little interest in industry for JTM and recommended further work be suspended. [Ref. SC21 N 4603 1990] Nevertheless, the reassessment report for JTM Full Class [SC21 N 4679 Revised] recommended completion of the International Standard texts, given the advanced state of the work. The recommendation was approved by SC21 in June 1990 [Ref. IST/21: 2160 1990].

The current versions of JTM are as follows:

- ISO/IEC 8831:1992, *Job Transfer and Manipulation Concepts and Services*, Edition 2, March 1992
- ISO/IEC 8832:1992, *Specification of the Basic Class and Full Protocol for Job Transfer and Manipulation*, Edition 2, March 1992.

9.11.9 Distributed Transaction Processing

9.11.9.1 Description of TP

OSI Distributed Transaction Processing (TP) supports a set of logically related operations affecting interrelated data and other resources across separate open systems in which the transaction is not simply an exchange of messages but in which the exchanges form a protected and indivisible set of messages. OSI TP operations are characterized by the four ACID properties supported by CCR (see Section 9.11.3.2): atomicity, consistency, isolation, and durability. [Ref. IGOSS 1993]

The TP protocol makes use of the facilities of the Commitment, Concurrency, and Recovery (CCR) application service element (ASE) and the Association Control Service Element (ACSE) (see Section 9.11.3). *It acts as a mediator for these protocols and operates in an* environment of many communicating pairs over many application associations. On the other hand, CCR and ACSE operate in a single peer-to-peer environment. As a mediator, TP does not specify any style of data transfer. It does provide an environment for an ASE to transfer data. It is up to a TP application to determine its user-ASE(s) to transfer data. Although there are user-ASEs such as Remote Procedure Call (RPC; see Section 9.11.3.5) and RDA (see Section 6.2.3) that can operate with TP, one can define a user-ASE that is specific for a TP application.

The user requirements addressed by ISO 10026 are to:

- Define procedures that support distributed transactions in order to:
  - Allow a distributed transaction to be organized into a transaction tree
  - Provide multi-party coordination, including local resources
  - Allow restoration to a consistent state, following failure of the state/context of a distributed transaction and of distributed information
  - Allow the detection of failure to achieve consistency
  - Allow a distributed transaction to be restarted following successful state restoration
  - Indicate successful completion or failure of a transaction
- Provide for the delimitation of a sequence of logically related transactions
- Allow the grouping of transactions within an applications process
- Allow for access control, access control granularity on groups of TP objects, authentication, and non-repudiation

- Allow conformance testing of the protocol and delineate clearly the static and dynamic conformance requirements (through a PICS statement).

9.11.9.2 TP Concepts and Options

A number of concepts are contained in TP in the areas of transaction categories, control modes, transaction types, and roles. These concepts illustrate some of the TP options and may be described as follows [Ref. IGOSS 1993]:

- Categories of transaction
  - Application-supported transactions—Allows two systems to communicate using a TP Dialogue. The ACID properties are the responsibility of the end user.
  - Provided-supported transactions—Allows two systems to communicate using all the TP functions. The ACID properties are the responsibility of the TP service provider.
- Control modes
  - Shared control—A mode that does not explicitly control the exchange of messages. Message exchange is based solely on the internal semantics of the programs, and they may use the TP Dialogue at their discretion. The TP service provider does not care about, nor is it aware of, any message collisions.
  - Polarized control—A mode that controls the exchange of messages between the two systems via a token. Under normal conditions, a system can use the TP Dialogue only if it has the token—TP will enforce this requirement. Under extraordinary circumstances, such as an abort, either system can use the Dialogue.
- Transaction types
  - Chained transaction—A series of related transactions, such as a batch of accounts receivable transactions, which start and continue until the batch ends. The sequence of events is that the first transaction builds the transaction tree, uses it, and either commits or rolls back; the second transaction uses the transaction tree and either commits or rolls back; and the third-to-the-last transactions each follows the same pattern. After the last transaction, the transaction tree is disbanded.
  - Unchained transaction—A transaction that establishes a transaction tree and communications with another program. Sometime during the communications, it is determined that a transaction should occur. That portion of the communication would be placed under the ACID properties and be recoverable by OSI TP. The transaction starts and completes with either a commit or roll back. The transaction tree may or may not be disbanded; if it remains, it is ready for the next transaction.
  - None (application supported)—In the case of the application-supported category of transactions, there is an undefined relationship between two systems—how a transaction starts and ends is an end-user concern.
- Roles for transactions
  - General transaction role—The system performs the task of the root node. It starts a transaction, and all participants in the transaction are its machines.
  - Responder transaction role—A system may only be a leaf on a transaction tree. It responds to a request to join a transaction and may not delegate any tasks to another system—it can only respond. A large database server might be an example.
  - General transaction role—A system may be a root, intermediate, or leaf node depending on how it is used at a specific time. This is the most robust and general-purpose product that could be procured and that can serve any role.

9.11.9.3 TP Standards

ISO/IEC 10026, *OSI Distributed Transaction Processing*, comprises the following parts:

- ISO/IEC 10026-1, Part 1: *Model*, December 1992 [SC21 N 7457] (X.860:1992)
  - PDAM 1, Amendment 1: *Commitment Optimization*, September 1993 [SC21 N 8219, 8220, 7649) (DAM expected June 1994; and AM expected June 1995)
- ISO/IEC 10026-2, Part 2: *Service*, August 1992 [SC21 N 7304] (X.861:1992)
  - PDAM 1, Amendment 1: *Commitment Optimizations*, September 1993 [SC21 N 8220]
- ISO/IEC 10026-3, Part 3: *Transaction Processing Protocol Specification*, December 1992 [SC21 N 7518] (X.862)
  - PDAM 1, Amendment 1: *Commitment Optimizations*, September 1993 [SC21 N 7649]
- ISO/IEC 10026-4, Part 4: *PICS Proforma*, SC21/WG5, October 1993 [SC21 N 8290] (X.863)
- ISO/IEC 10026-5, Part 5: *Application Context Proforma*, 1993
- ISO/IEC 10026-6, Part 6: *Unstructured Data Transfer*, 1993
- CD 10026-7, Part 7: *Message Queueing*, July 1993 [SC21 N 8148] (DIS text expected early in 1994).

In addition to the CD-level amendments (PDAMs) on commitment optimizations cited above, the following working draft amendments (WDAMs) apply to Parts 1-3:

- *Distributed Transaction Processing Dialogue Recovery and User Suspension of a Dialogue* [SC21 N 6710] (PDAMs expected November 1995, DAMs November 1996, and AMs November 1997)
- *Transaction Processing Association Pool Management*, February 1992 [SC21 N 7604] (formerly entitled Association Management) (PDAMs expected July 1994, DAM July 1995, and AM July 1996)
- *Transaction Processing Sub-Transactions*, SC21/WG5, July 1991 [SC21 N 6236] (PDAMs expected November 1995, DAMs November 1996, and AMs November 1997)
- *Transaction Processing Separate Data and Commit Associations*, July 1991 [SC21 N 6240] (PDAMs expected November 1995, DAMs November 1996, and AMs November 1997)
- *Transaction Processing Security*, July 1991 [SC21 N 6232] (PDAMs expected November 1995; DAMs November 1996; and AMs November 1997).

CD 11587.2 is the second draft of a standard for *Application Content for Systems Management with Transaction Processing*, July 1993 [SC21 N 7899] (editing meeting February 1994; initiation of ITU-TS approval ballot expected June 1995) (X.702).

Significant changes to the TP model (ISO 10026-1) made in December 1990 were removal of dynamic switching between chained and unchained transactions, thus enabling conforming systems to implement any one of three modes of operation: application-supported transaction, provider-supported chained transaction, and provider-supported unchained transaction. Provided-supported chained transactions require that each transaction within a dialogue use full two-phase commit procedures (CCR), while provided-supported unchained transactions always start with application-supported transactions (no CCR) with an explicit request for two-phase commit support for each transaction that requires provider-supported commitment.

The TP protocol document (ISO 10026-3) has been restructured into a form intended to be more easily understood with simpler descriptive techniques. In addition, there were changes to simplify and correct protocol procedures. Special care was given to the two-phase commit protocol and its use of CCR services to ensure that all collision cases were resolved. [Ref. SC21 N 5603 1990] ISO 10026-3 does not provide a data transfer facility, leaving the TP user free to choose a data transfer paradigm that best suits the user's needs.

Unstructured Data Transfer (UDT) for OSI Transaction Processing (ISO 10026-6) allows interconnection of computer systems from different manufacturers, including those under different management; of different levels of complexity; and of different technologies. UDT is not suitable outside the TP environment.

The new work item accepted by JTC1 for *Other Data Transfer for OSI TP* has been retitled *Message Queueing* (CD 10026-7). Included in the scope of this work is development of TP queue services that would support transactions broken down into multiple steps. These services could also be used as the basis for a deferred transaction initiation mechanism or as a mechanism for reliable message transfer. [Ref. SC21 N 5184 1990] ISO status is expected in November 1994.

ISO 10026 will be used by the RDA standard and is being considered for use by RPC, extensions to IRDS, and extensions to FTAM. It is the first Application Layer service for distributed processing. [Ref. SC21 N 4759 1990]

TP is dependent on a revised version of CCR that was progressed in 1989. Two formal descriptions of TP have been produced, one each in Estelle and LOTOS; both will be progressed as informative annexes to the TP protocol. TP activity will be conducted in coordination with work on RDA (SC21/WG3) and Application Layer standards (SC21/WG6).

9.11.9.4 TP Profiles

The ISP for TP (ISO/IEC 12061) specifies the options (interoperability parameters) required to build a conformant TP application. It specifies not only how the TP and CCR base standards are used but also how to construct conformant Application, Presentation, and Session Layers for interconnection.

ISO/IEC 12061, *ISPs ATP nn - OSI Distributed Transaction Processing*, has the following 13 parts, of which the first 8 have reached DIS status:

- DISP 12061-1, Part 1: *Introduction*, 1993
- DISP 12061-2, Part 2: *Support of the OSI TP APDUs*, 1993
- DISP 12061-3, Part 3: *Support of the CCR Protocols*, 1993
- DISP 12061-4, Part 4: *Support of ACSE, Presentation and Session Protocols*, 1993
- DISP 12061-5, Part 5: *ATP 11, Application Supported Transactions with Polarized Control*, 1993
- DISP 12061-6, Part 6: *ATP 12, Application Supported Transactions with Shared Control*, 1993
- DISP 12061-7, Part 7: *ATP 21, Provider Supported Transactions in Unchained Mode with Polarized Control*, 1993
- DISP 12061-8, Part 8: *ATP 22, Provider Supported Transactions in Unchained Mode with Shared Control*, 1993
- pDISP 12061-9, Part 9: *ATP 31, Provider Supported Transactions in Chained Mode with Polarized Control*, 1993

- pDISP 12061-10, Part 10: *ATP 32, Provider Supported Transactions in Chained Mode with Shared Control*, 1993
- pDISP 12061-11, Part 11: *TP Transaction Recovery Application Context*, 1993
- pDISP 12061-x, Part x: *Systems Profiling for TP*, 1993
- pDISP 12061-y, Part y: *Development of PTS for TP*, 1993
- EWOS/TA/93/083, *ISP FDI 41, Directory Data Definitions - Use of Directory for OSI TP*, Part 1: *Basic Naming and Addressing*, October 1993
- EWOS/TA/93/084, *ISP FDI 42, Directory Data Definitions - Use of Directory for OSI TP*, Part 2: *Enhanced Naming and Addressing*, October 1993.

9.11.9.5 TP New Work Items

Table 28 identifies the new work items that have been proposed for TP. Work has begun on TP association pool management (formerly called association management). It is WD 10026-x, *TP Association Pool Management Function*, Working Draft, SC21 N 7604, 2 February 1993. Association management is concerned with manipulation and query of management information corresponding to an association and its relationships with supporting connections. [Ref. SC21 N 7417 1992]

Table 28. New Work Items Proposed in ISO for TP

- TP Association Pool Management—to provide for the management of application associations in a distributed processing environment involving multiple open systems [SC21 N 5177]. Old title was TP Association Management. WD 10026-x, TP Association Pool Management Function [SC21 N 7604, February 1993]
- TP Dialogue Recovery—the third phase of recovery (as defined in ISO 10026-1); it is required to enable Transaction Processing Service User Invocations (TPSUIs) to continue normal operation following the re-establishment of bound data consistency [SC21 N 4170]. A WD was produced in January 1992 [SC21 N 6710]. CD text was expected in June 1993, DIS in June 1994, and IS in June 1995.
- TP Heuristic Decisions—provides advisory propagation of a heuristic decision to all nodes; advisory propagation to nodes in the subtree below the node taking the heuristic decision; mandatory propagation of a heuristic decision to all nodes; and mandatory propagation to nodes in the subtree below the node taking the heuristic decision [SC21 N 4167]. PROJECT CANCELLED in June 1993.
- TP Savepoints—service to enable a transaction to be able to save and later restore a consistent state of all bound data under its control [SC21 N 4171]; new work item not accepted by JTC1, June 1990.
- TP Security—considers requirements for provision of a secure environment for TP in areas such as access control, auditing, authentication, confidentiality, integrity, management, nonrepudiation, replay, and revocation [SC21 N 5176, approved June 1990]. In the absence of an Editor and WD, SC21 is recommending cancellation of this project.
- TP Subtransactions -extensions to TP that would provide partial rollback and nested transactions [SC21 N 6236]. In the current TP standard (ISO 10026), all the bound data that are involved in a transaction tree for a transaction are committed together and, if the transaction fails, all the bound data are rolled back. In the absence of an Editor and WD, SC21 is recommending cancellation of this project.
- TP Separate Data and Commit Associations - [SC21 N 6240, 31 May 1991]. Amendments to Parts 1, 2, 3, and 4. PDAMs expected June 1994, DAM in June 1995, and AM in June 1996. SC21 N 7166, May 1992, Requirements and Issues for the Separation of Data and Commit Flows in OSI-TP.
- TP Conformance Testing. A two-part standard. WD on Test Suite Structure and Test Purposes (TSSTP) [SC21 N 8216]. Second part is Test Management Protocol (TMP).

Sources: [Ref. Bainbridge 1989, SC21 WG5 N 673 1992]

An *Association Pools Requirements and Requirements Issues* [SC21 N 6698] document was the output of discussions held at the TP Rapporteur's meeting in November 1991. The *Discussion Paper on Association Pools as an Extension of ACSE*, April 1991 [SC21 N 5835], provides a possible overall approach for the NWI covering TP Association Pool Management. A

discussion paper, *Strawman Design: TP Association Pools* [SC21/WG5 N 660], was issued in May 1992 to progress the work. SC21/WG6 has identified a number of issues related to the project that are discussed in [SC21 N 7168, June 1992].

A new work item on TP security [SC21 N 6232, July 1991] is intended to expand the TP model, service, and protocol (ISO 10026-1,2,3) to provide a secure environment for distributed transaction processing interactions involving multiple open systems. PDAD text is expected in 1993, DAD in 1994, and AD in 1995. In a March 1992 communication to WG5 [SC21/WG5 N 653], the United States suggested that in light of the Security Exchange Service Element (SESE) being defined by WG6 (see Section 11.2.2.4) it is unnecessary to develop a complete TP Security Model, as many of the security threats perceived by users of OSI TP may be counteracted Suites. Thus, the United States proposed that the TP Security Model be refined to only reflect the security services that need to be provided directly by OSI TP, namely entity authentication, access control, and non-repudiation. In the absence of an Editor and WD, SC21 is recommending cancellation of the project.

In September 1993, WG5 issued a revised *Working Draft for a Conformance Test Suite for the TP Protocol, Part 1, Test Suite Structure (TSS) and Test Purposes (TP)* [SC21 N 8216] for study and comment. This NWI was accepted into the JTC1 work program and an Initial Abstract Test Suite for TP was produced in November 1992. [Ref. SC21 N 7676 1993] Part 2 is TP Test Management Protocol (TMP).

Two approaches are being considered for using RPC and TP together [Ref. SC21 N 5172 1990]:

- With RPC as the data transfer paradigm for TP, with use being made of TP dialogue management functions
- Using TP commitment functionality to complement the operation of RPC-based services (without necessarily making use of TP dialogues) to support "exactly once" semantics.

A liaison paper on TP with RPC [SC21 N 8067] was distributed in July 1993, which called for comments on the integration of RPC with TP, since many users need an RPC with transactional semantics. In October 1993, the US response to this paper suggested that instead of beginning a new standardization effort for transactional RPC, SC21/WG8 may wish to fast-track X/Open's TxRPC specification. TxRPC is an interface to a communications resource manager that is predicated on the use of OSI TP.

In 1989 a potentially serious problem was identified for TP. Under certain circumstances, protocol exchanges from one transaction (such as rollback) could overtake those outstanding from a previous transaction (and could therefore be interpreted by the receiving node as pertaining to the previous transaction). This can occur if lower layer expedited services are used to convey particular PDUs. The interim solution that was adopted was to avoid the use of Transport expedited data transfer services. This issue has raised the possible requirement for a Non-Blocking Transport Expedited Service. A June 1991 US Expert's Paper [SC21/WG4 N 721] outlined one solution for non-blocking transport expedited service. However, the TP Rapporteur Group believes that such a service is unnecessary and undesirable because of its effects on dependent upper layer services. [Ref. SC21 N 7175 1992]

In October 1993, the US national body identified a requirement for partial roll back of a transaction within the OSI TP, wherein a transaction's branches may be rolled back in a transaction

that is eventually committed. Branches may need to be rolled back as a result of either the occurrence of certain types of branch failure or from requests by superior nodes to undo branch operations. [Ref. SC21 N 8321 1993]

9.11.10 OSI Information Retrieval (IR)[54]

The OSI Information Retrieval (IR) application supports the open interconnection of information clients with information servers by specifying an OSI application layer protocol for intersystem search and retrieval of information. IR addresses retrieval (but not update) of information, and the IR protocol specifies basic information retrieval operations, a common syntax for queries and the means to express their semantics, and the means to allow the partner systems to share an understanding of the information retrieved. The IR protocol provides access to information resources without requiring servers to structure databases similarly or to name fields within record structures similarly. It provides the means to register attribute set definitions that express the semantics of information exchanged. The standard supplies a basic attribute set for search and retrieval of text-based information.

The standards for IR are the following:

- ISO/IEC 8777, *Information and Documentation - Commands for Interactive Text Searching*, 1993
- ISO/IEC 10162, *Information and Documentation - Search and Retrieve Application Service Definition for Open Systems Interconnection*
- ISO/IEC 10163, *Information and Documentation - Search and Retrieve Application Protocol Specification for Open Systems Interconnection*
- ANSI Z39.50-MA-26, *Implementor's Group Profile.*

Profiles for IR need to specify such options as whether it applies to the client, the server, or both.

9.12 Internetworking

9.12.1 General Interworking Standards

The basic interworking standards used for specifying relays are the following (examples of relay profiles using these standards are given in Appendix B):

- ISO/IEC 10028-1, *Definition of the Relaying Functions of a Network Layer Intermediate System*, Part 1: *Connection-mode Network Service*, 1993
  - PDAM 1, *Connectionless Mode Relaying Functions*, February 1991
- ISO/IEC 10028-2, *Definition of the Relaying Functions of a Network Layer Intermediate System*, Part 2: *Connectionless Network Service*, 1993
- ISO/IEC TR 10029, *Operation of an X.25 Interworking Unit*, March 1989
- ISO/IEC 10030, *End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO/IEC 8878 (X.25 PLP)* [SC6 N 5006], October 1990
  - PDAM 1, *Dynamic Discovery of OSI NASP Addresses by End Systems*
  - AM 2, *PICS Proforma*, 1992 (see DIS 10030-2)
  - PDAM 3, *Specification of IS-SNARE Interactions*, August 1991

[54] This section is based on excerpts from [IGOSS 1993].

- DIS 10030-2, *End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO/IEC 8878 (X.25 PLP)*, Part 2: *PICS Proforma*, October 1991
- DIS 10038, *Local Area Networks - MAC Sublayer Interconnection (MAC Bridging)* (awaiting DIS ballot), December 1991
  - PDAM 1, *Specification of Management Information for CMIP*
  - DAM 2, *Source Routing Supplement*, October 1991
- ISO/IEC 10177, *Intermediate-System Support of the OSI Connection-Mode Network Service Using ISO 8208 in Accordance with ISO 10028*
- ISO/IEC 10589, *Intermediate System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8473*
- DIS 10747, *Protocol for Exchange of Inter-Domain Routing Information Among Intermediate Systems to Support Forwarding of ISO 8473 PDUs.*

ANSI X3S3 has three MAC-related liaison projects with JTC1/SC6 underway:

- To develop a technical report that will provide a description of the representation of MAC Addresses. The report will record all values assigned for the use of Standards in one document, whereas at present this information is scattered across a number of documents. [Ref. X3 1991b]
- To develop an amendment to DIS 10038 that will extend the scope to include source routing capability. [Ref. X3 1991c]
- To develop a technical report that will provide guidelines for LANs implementing "source routing operation" defined in DIS 10038/DAM 2, *MAC Bridging - Source Routing Supplement*, October 1991. [Ref. X3 1991d]

TR 10172, *Network/Transport Protocol Interworking Specification*, October 1990 [SC6 N 5906, March 1990], addresses the inability of end systems operating in the CO network protocol (ISO 8208/8878 X.25) and CL network protocol (ISO 8473) to interwork with each other. A mediating device, called the Interworking Functional Unit (IFU), is defined to perform relaying and/or conversion of protocol data units (PDUs) from one network protocol type to another. Three modes of operation are considered in TR 10172:

- <u>Network Layer Relay (NLR)</u>. In the NLR mode the IFU operation functions as a regular intermediate system. CL NLR operation is in accordance with ISO 8473 and CO NLR with ISO 10177 and ISO 10028.
- <u>Passive Transport Layer Relay (PTLR)</u>. PTLR does not itself operate on the PDUs of transport connections, but passes transport PDUs received in network service data units from each end system transparently to the other end system.
- <u>Active Transport Layer Relay (ATLR)</u>. ATLR provides an end-to-end transport service by operating a separate transport connection to each of the connected end systems and relaying data from one connection to the other.

Since the PTLR and ATLR modes of operation lie outside the scope of the OSI architecture, the technical report is not planned to be converted to an ISO standard.

Network Relay (also called Routing), however, is the most important outstanding issue in the Network Layer. The standards that describe the protocols and algorithms for routing over a connectionless network service have progressed rapidly over the last 3 to 4 years, after a slow start, but final standards and products that implement them have started appearing. The equivalent work on routing for connection-oriented networks has proceeded more slowly, and it is not clear when draft standards will be published. Examples of network relay profiles appear at the end of

Appendix B. Four OSI standards are of particular importance to the provision of open routing [Ref. OSN 1990b]:

- ISO 8473, *Protocol for Providing Connectionless-Mode Network Service*
- ISO 9542, *End System to Intermediate System (ES-IS) Routing Exchange Protocol*
- ISO/IEC 10589, *Intermediate System to Intermediate System (IS-IS) Intra-domain Routing Exchange Protocol*, 1992
- DIS 10747, *Protocol for Exchange of Inter-domain Routing Information Among Intermediate Systems to Support Forwarding of ISO/IEC 8473 PDUs*, 1993

EWOS has released a *Technical Guide to Routing in the Context of OSI*, EWOS-EGLL/91/72 [IST/21:2860], May 1991.

Task Group ANSI X3S3.7 of Accredited Standards Committee (ASC) X3S3, Data Communications, is developing a draft standard describing the interworking between two packet switched data networks (PSDNs) via an X.25 link. This draft standard (Project 682-D) would typically be used for interworking between a packet switched public data network (PSPDN) and a packet switched private data network (PSPvtDN). It specifies the general addressing and routing principles associated with two PSDNs and their interworking as well as the procedures to be followed by an interworking function (IWF) that is used to connect the PSPDN and the PSPvtDN. [Ref. X3 1991e]

The following comment on CL-mode and CO-mode interworking was provided to SC21 following a February 1990 meeting of ITU-TS SG VII regarding the proposed update to the OSI Reference Model (ISO 7498-1) [Ref. SC21 N 4559 1990]:

> *The connectionless/connection-mode crossover rules currently proposed by ISO appeared, to many of the Q23/VII attendees at this meeting, to be unacceptable for use in fully supporting connectionless-mode ITU-TS applications, due mainly to interconnectivity problems. Many of the attendees felt that, for "across-the-board" support of connectionless ITU-TS applications, within the lower layers, there is a need to have common (mandatorily provided) support required that would assure interconnectivity among all connectionless-mode OSI ITU-TS applications. It was unanimously agreed that the concept of attempting to solve such interconnection problems exclusively through introduction of any "transport relay" concept in ITU-TS Recommendations is totally unacceptable.*

Technical Committee, ANSI X3.T6, Non-Contact Information Systems Interface (NCISI), is developing a non-contact standard interface between computer devices for the transfer of information. The committee is developing a standard for US activities; however, it eventually intends the standard to be submitted to ANSI as a JTC1 Fast Track Candidate for approval as an international standard. The committee will review current technology in radio frequency data/communication, infrared, and similar non-contact data transfer technologies with the objective of standardizing the interface between like devices. The standard would be restricted to the interface, allowing unrestricted development of computer components on either side of the interface. [Ref. X3 1991f]

Task Group X3S3.7 of ASC ANSI X3S3, Data Communications, has begun an effort to develop a standard to be used in conjunction with frame relay standards. It could be used in other cases where X.25 virtual circuit (VC) establishment and clearing procedures and other non-VC-specific procedures are not needed. This standard will be a subset of Recommendation X.25 and ISO 8208. [Ref. X3 1991g]

9.12.2 Relay ISPs (R-Profiles)

Table 29 lists the relay profiles currently being standardized by ISO as ISPs.

Table 29. Relay Profiles Standardized by ISO

DISP 10612-1	ISPs RD nn.nn, Part 1: RD 5p.5q Profile, Relaying MAC Using Transparent Bridging - General Overview and Subnetwork-Independent Requirements, 1993
DISP 10612-2	ISPs RD nn.nn, Part 2: RD 5p.5q Profile, Relaying MAC Using Transparent Bridging - CSMA/CD LAN Subnetwork-Dependent Media-Independent Requirements, 1993
pDISP 10612-3	ISPs RD nn.nn, Part 3: RD 5p.5q Profile, Relaying MAC Using Transparent Bridging - CSMA/CD LAN Subnetwork-Dependent Media-Dependent Requirements, 1993
DISP 10612-4	ISPs RD nn.nn, Part 4: RD 51.51 Profile, MAC Service Relay Using Transparent Bridging, CSMA/CD LAN - CSMA/CD LAN, 1993
pDISP 10612-5	ISPs RD nn.nn, Part 5: RD 51.54 Profile, MAC Service Relay Using Transparent Bridging, CSMA/CD LAN - FDDI LAN, 1993
pDISP 10612-6	ISPs RD nn.nn, Part 6: RD 54.54 Profile, MAC Service Relay Using Transparent Bridging, FDDI LAN - FDDI LAN, 1993
pDISP 10612-7	ISPs RD nn.nn, Part 7: RD 51.53 Profile, MAC Service Relay Using Transparent Bridging, CSMA/CD LAN - Token Ring LAN, 1993
pDISP 10612-8	ISPs RD nn.nn, Part 8: RD 53.53 Profile, MAC Service Relay Using Transparent Bridging, Token Ring LAN - Token Ring LAN, 1993
pDISP 10612-9	ISPs RD nn.nn, Part 9: RD 53.54 Profile, MAC Service Relay Using Transparent Bridging, Token Ring LAN - FDDI LAN, 1993
pDISP 10613-1	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 1: Relay Function, Overview, Subnetwork-Independent Requirements, 1993
pDISP 10613-2	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 2: LAN Subnetwork-Dependent, Media-Independent Requirements, 1993
pDISP 10613-3	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 3: CSMA/CD LAN Subnetwork-Dependent Media-Dependent Requirements, 1993
DISP 10613-4	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 4: FDDI LAN Subnetwork-Dependent Media-Dependent Requirements, 1993
pDISP 10613-5	ISPs RA nn.nn -Relaying the Connectionless-mode Network Service, Part 5: RA51.51 Profile, CSMA/CD LAN - CSMA/CD LAN, 1993
pDISP 10613-6	ISPs RA nn.nn -Relaying the Connectionless-mode Network Service, Part 6: RA51.54 Profile, CSMA/CD LAN - FDDI LAN, 1993
pDISP 10613-7	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 7: PSDN Subnetwork Media Dependent VC Permanent Access, 1993
pDISP 10613-8	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 8: RA51.1111 Profile, 1993
pDISP 10613-9	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 9: RA51.1121 Profile, 1993
pDISP 10614-1	ISPs RC nn.nn - Relaying X.25 PLP, Part 1: General Overview and Subnetwork Independent Requirement, 1993
pDISP 10614-2	ISPs RC nn.nn - Relaying X.25 PLP, Part 2: LAN Subnetwork Dependent Media Independent Requirement, 1993
pDISP 10614-3	ISPs RC nn.nn - Relaying X.25 PLP, Part 3: CSMA/CD LAN Subnetwork Dependent Media Dependent, 1993
pDISP 10614-4	ISPs RC nn.nn - Relaying X.25 PLP, Part 4: PSDN Subnetwork Type Dependent Requirement, 1993
DISP 10614-5	ISPs RC nn.nn - Relaying X.25, Part 5: RC51.1111, CSMA/CD - PSDN Permanent Access PSTN-Leased Virtual Circuit, 1993
DISP 10614-6	ISPs RC nn.nn - Relaying X.25, Part 6: RC51.1121, CSMA/CD - PSDN Permanent Access CSDN-Leased Virtual Circuit, 1993.

9.12.3 Routing (Transport) ISPs (T-Profiles)

Table 30 lists the relay profiles currently being standardized by ISO as ISPs. Because of the large number (48) of parts to ISP 10609, the table shows only Parts 1-14 and those parts beyond Part 14 that have reached DISP status. Others may be found in Appendixes D and E.

Table 30. Transport Profiles Standardized by ISO

ISO/IEC ISP 10608-1	ISPs TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service (COTS over CONS), Part 1: General Overview and Subnetwork-Independent Requirements, 1992
ISO/IEC ISP 10608-2	ISPs TA nnnn - COTS over CONS, Part 2: TA51 Profile Including Subnetwork-dependent Requirements for CSMA/CD Local Area Networks, 1992
DISP 10608-3	ISPs TA nnnn - COTS over CONS, Part 3: TA 52, LAN, Token Bus: CLNS
ISO/IEC ISP 10608-4	ISP TA nnnn - COTS over CONS, Part 4: TA53 COTS over CLNS, LICI, Token Ring LAN
ISO/IEC ISP 10608-5	ISPs TA nnnn - COTS over CONS, Part 5: TA1111/TA1121 Profiles Including Subnetwork-dependent Requirements for X.25 Packet Switched Data Networks Using Switched Virtual Circuits, 1992
DISP 10608-6	ISPs TA nnnn - COTS over CONS, Part 6: TA54 Profile
DISP 10608-13	ISPs TA nnnn - COTS over CONS, Part 13: LAN-Dependent Requirements for Token Ring MAC and PHY
DISP 10608-14	ISPs TA nnnn - COTS over CONS, Part 14: MAC, PHY, PMD Sublayer Dependent State Management Requirement Over FDDI LAN Subnetwork
ISO/IEC ISP 10609-1	ISPs TB, TC, TD, and TE - COTS over CONS, Part 1: Subnetwork-type Independent Requirements for Group TB, 1992
ISO/IEC ISP 10609-2	ISPs TB, TC, TD, and TE - COTS over CONS, Part 2: Subnetwork-type Independent Requirements for Group TC, 1992
ISO/IEC ISP 10609-3	ISPs TB, TC, TD, and TE - COTS over CONS, Part 3: Subnetwork-type Independent Requirements for Group TD, 1992
ISO/IEC ISP 10609-4	ISPs TB, TC, TD, and TE - COTS over CONS, Part 4: Subnetwork-type Independent Requirements for Group TE, 1992
ISO/IEC ISP 10609-5	ISPs TB, TC, TD, and TE - COTS over CONS, Part 5: Definition of Profile TB 1111/TB 1121, 1992
ISO/IEC ISP 10609-6	ISPs TB, TC, TD, and TE - COTS over CONS, Part 6: Definition of Profile TC 1111/TC 1121, 1992
ISO/IEC ISP 10609-7	ISPs TB, TC, TD, and TE - COTS over CONS, Part 7: Definition of Profile TD 1111/TD 1121, 1992
ISO/IEC ISP 10609-8	ISPs TB, TC, TD, and TE - COTS over CONS, Part 8: Definition of Profile TE 1111/TE 1121, 1992
ISO/IEC ISP 10609-9	ISPs TB, TC, TD, and TE - COTS over CONS, Part 9: Subnetwork-type Dependent Requirements for Network Layer, Data Link Layer, and Physical Layer Concerning Permanent Access to a Packet Switched Data Network Using Virtual Call, 1992
pDISP 10609-10	ISPs TB, TC, TD, and TE - COTS over CONS, Part 10, 1993
pDISP 10609-11	ISPs TB, TC, TD, and TE - COTS over CONS Part 11, 1993
pDISP 10609-12	ISPs TB, TC, TD, and TE - COTS over CONS, Part 12: TC51 Profile, 1993
pDISP 10609-13	ISPs TB, TC, TD, and TE - COTS over CONS, Part 13: TC53 Profile, 1993
pDISP 10609-14	ISPs TB, TC, TD, and TE - COTS over CONS, Part 14: COTS Classes 0 and 2, CONS, LLC2, Token Ring LAN, 1993
DISP 10609-31•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 31: TC 1231, ISDN B-Channel Virtual Call, Switched Access to a PSDN, 1993
DISP 10609-32•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 32: TC 4111, ISDN B-Channel X.25 DTE to DTE, Semi-permanent Service, 1993
DISP 10609-33•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 33: TC 4112, ISDN B-Channel X.25 DTE, Circuit-mode Service, 1993
DISP 10609-34•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 34: TC 43111, ISDN D-Channel Access Virtual Call, Packet-mode Service, Without Q.931, 1993
DISP 10609-35•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 35: TC 43112, ISDN D-Channel Access Virtual Call, Packet-mode Service, with Q.931, 1993
DISP 10609-36•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 36: TC 43211, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, Without Q.931, 1993
DISP 10609-37•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 37: TC 43212, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, with Q.931, 1993
DISP 10609-38•	ISPs TB, TC, TD, and TE - COTS over CONS, Part 38: TC 4331, ISDN B-Channel Demand Access Virtual Call, Packet-mode Service, 1993

Note: pDISPs 10609 (Parts 20-30 and 40-48) are omitted from this table but included in Section I.H of Appendix D and in Appendix E (only the those parts beyond Part 14 that have reached DISP status are shown in the table).

9.13 Other Standards and Issues

9.13.1 Time Synchronization

ITU-TS SG VII(Q19) has begun work on a time synchronization service (TSS). The work is based on the US DoD RFC-1119, *Network Time Protocol (NTP)*, currently being used by the Internet community (see Section 9.7.4). The TSS time standard is based on the Coordinated Universal Time (UTC), determined by the Bureau International de l'Heure (BIH) from astronomical observations provided by the US Naval Observatory and other observatories.[55]

The TSS can be used in distributed systems in several ways: to measure elapsed time, to preserve the order of events, and to coordinate activities of a set of processes. The elements of the TSS model are the following:

- Local clock—an oscillator that, once set with a time value, attempts to maintain a local estimate of global time
- Time user agent (TUA)—the user of the TSS
- Time synchronization agent (TSA)—the provider of the service.

Each TUA interacts with a set of TSAs to obtain information, from this information to determine the best estimate of global time, and to set the local clock to this value. The TUA may adjust the frequency of the local clock to compensate for drift in the hardware. Synchronization of clocks is by continuous distribution of time—TUAs build up information based on samples of a number of servers for the delay characteristics of the communication path between itself and each of the TSAs.

Time is distributed through the system via a hierarchical set of TSAs. Stratum 1 TSAs, at the top of the hierarchy, have local clocks that are set by external means from the most accurate sources available. These means could include radio receivers and such satellite devices as the Global Positioning System. Clocks that have been set by TUAs that have obtained time information directly from Stratum 1 TSAs are said to be at Stratum 2. At each level of the hierarchy, except the top and bottom, each TUA may have an associated TSA that can be used to distribute time information in the local clock to TUAs at the next lower level of the stratum. It is expected that there will be a number of Stratum 1 TSAs, some being provided as public services. Each site using LANs would have two or more Stratum 2 TSAs, and each LAN segment could have two or more Stratum 3 TSAs. Individual end systems might not need to have clocks at much more than Stratum 4. [Ref. SC21 N 4565 1990]

A task force has been set up under ISO/TC184/SC5/WG2 to look at the requirements for a time-critical communications architecture (TCCA) because the network architectures set up so far are primarily intended for general traffic and are not always capable of providing adequate performance and resilience for time-critical communications, especially where time-critical and non-time-critical traffic coexist. In particular, in many CIM and control installations there appears to be a requirement for an intermediate network, between general enterprise-wide networks (e.g., MAP) and field-bus-type networks. This intermediate network would carry both bulk data transfers and time-critical messages, and be able to operate over considerable distances and in hostile environments. A liaison between TC184/SC5/WG2 and SC21/WG4, OSI Management [Ref. SC21 N 5602 1991] has been established. ANSI X3.102, *Data Communication Systems*

[55] Discussion on time synchronization was taken from SC21 N 4565, *Liaison Statement to SC21/WG4/WG7 on Time Synchronization*, CCITT SG VII, March 1990.

and Services User Oriented Performance Parameters, 1983, Revised 1990, is being used as a basis for the effort. A key requirement of a TCCA is a set of services aligned with ISO/IEC, MMS (see Section 9.11.5). One aspect of Time-Critical Communications Systems (TCCS) is Time Synchronization.

In May 1992, SC21/WG1 posed a new question (Q1/65) on user requirements for OSI systems supporting time critical communications. The question is, what architectural enhancements to ISO 7498, if any, are required to meet the requirements of the TCCA? The Technical Report of the TTCA rapporteurs group of TC184/SC5/WG2 identifying user requirements for systems supporting time critical communications (TR 12178, December 1993) will be used as a basis for an answer. [Ref. SC21 N 7090 1992] The results of a ballot taken on this question clearly indicate that National Bodies support work on this proposed new question. Therefore, SC21/WG1 began work on Q1/65 in June 1993. [Ref. SC21 N 7467 1992]

MiniMAP is a simplified three-layer subset of the MAP specification intended for time-critical applications. The World Federation of MAP/TOP Users' Groups has agreed to adopt the Factory Automation Interconnection System (FAIS) to enhance the MiniMAP specification. The addition was expected to be part of an update to MAP version 3.0, known as MAP 3.0 (1993) so as not to be confused with the current MAP 3.0.

SC18/WG4 has proposed a new work item for a Coordinated Time Service in an OSI Environment. It proposes developing a two-part international standard that would specify an abstract service and protocol to provide the date and time of day in response to a request and provide synchronization of time between systems. WD status was expected in September 1992, CD in September 1993, DIS in September 1994, and IS in September 1995 [Ref. SC21 N 6749 1992]. This work item is relevant to the Time Management Function of Systems Management (WD 10164-tm, see Section 12.1.3.3). However, a WD is not available now because WG4 has not received substantial contributions. Moreover, the Australian NB wonders why this work should be progressed as a NWI by SC18 when SC18's "communication" standards only cover that of Store and Forward - X.400. In their view, the development of a "real time" time management system must be the responsibility of SC21. [Ref. SC21 WG4 N 1451 1992]

SC21/WG4, in a liaison statement to SC18/WG4 regarding this topic, states that the majority of the requirements of the Coordinated Time Services are within the scope of the Time Management Function (WD 10164-tm) (see Section 12.1.3.3). [Ref. SC21 N 7587 1993]

9.13.2 Transparent File Access (TFA)

IEEE P1003.8 is the draft TFA standard. TFA includes capabilities for managing files and transmitting data through heterogeneous networks in a manner that is transparent to the user. IEEE P1003.8 completed its first ballot in May 1992 and is expected to become a FIPS by mid-1993. [Ref. APP 1992] Chapter 7 discusses P1003.8 along with the other POSIX standards.

9.13.3 Efficiencies of OSI Protocols

ITU-TS SGVII and JTC1 (SC6 and SC21) are concerned with the efficiency of OSI protocols when used over long delay circuits such as satellite circuits. SGVII is currently evaluating three proposals in terms of their potential for efficiency improvement as well as in terms of the amount of changes they would require on architecture, services, and protocols across all OSI layers:

- Use of the data link level XID command (HDLC)
- Use of extended fast select packets
- Use of the proposed Forward Acting Strategy for Telecommunications (FAST).

SGVII intends to keep SC21 and SC6 informed of the progression of its studies. It held a special meeting on the topic in October 1992 during which approaches for a solution were discussed. Document SC21 N 7577 identifies two potential upper layer enhancements to improve the overall procedures for establishing communication between two application entity instances:

- Eliminate a protocol round trip when establishing an association
- Remove the blocking effect of the A-ASSOCIATE service.

The United States suggests fixed encoding as a third area for enhancing the general, overall efficiency of the upper layers. [Ref. SC21 N 7866 1993]

In June 1993, SC21/WG1 held a special meeting, with representatives from SG7 of ITU-TS, on the subject of efficiency of OSI protocols; the meeting was convened, in part, to respond to the liaison statement [SC21 N 7577] from SG7 in February 1993. The ITU-TS is considering the following approaches [Ref. SC21 N 8018]:

- Embedding connection establishment protocol data units (PDUs) at the Transport Layer. This is currently not allowed because the Session Layer can reuse a transport connection. Applications with well-known requirements in terms of initial application PDU sizes could make use of this approach. Selecting such applications and establishing a special mechanism for them would be similar to establishing an application-specific profile. Care needs to be taken to balance such an approach with other mechanisms. For example, creating large PDUs to avoid segmentation may introduce unacceptable delays if a relay operates in the path.
- FAST method. This proposal involves the architectural implications of expressing the concept of phases in the operation of a connection in the OSI Reference Model and whether the FAST concept violates this expression. If so, modifications to the OSI Reference Model would need to be studied.

SC6/WG4 has begun work on *Enhanced Communications Functions and Facilities (ECFF) for the Lower Layers (Layers 1-4)*. In addition, SC21/WG1 is looking at a Fast Connection Setup (FCS) feature, which is apparently consistent with the OSI Reference Model but would require some changes to service definitions (e.g., Transport Service). An approach to defining such a feature has been proposed in SG6/WG4 (reducing the number of handshakes required to set up a connection). Other approaches being discussed are termed FAST BYTE, HDLC XID (adds an I-field), and extended HDLC SABM (adds an information field). Some prefer the XID approach (Option 1 in HDLC) (e.g., SG8 in ITU-TS) and believe it possible to specify that approach with no revisions required in the OSI Reference Model. FAST BYTE [defined in CCITT COM VII-R-63(1992)] apparently requires little or no functionality at an OSI layer for a given communication and preserves OSI compatibility and compliance. This potentially should end the need for short stacks of OSI applications and allow for much greater compatibility for efficient communications among them, thus increasing the attractiveness of OSI. SG7 planned full discussions of these proposals at the February 1994 meeting.

9.13.4 Enhanced Transfer Mechanisms

The emergence of new high speed network technologies (e.g., for operation over fiber optic transmission facilities) and an expanded set of supporting requirements for applications (e.g., multicast operation and efficiency) have spurred interest in the development of enhanced

mechanisms in the lower four layers. SC6 is working on a project aimed at satisfying these needs. It will develop guidelines for the lower layers to support an enhanced transport mechanism that can include [Ref. SC6 N 6887 1991]:

- Very high data throughput capability for operation over high speed (e.g., 20 Mbps to 10 Gbps) transmission facilities
- Multicast operation to support multipeer applications
- Selectable error control procedures
- Enhanced QoS selection and management (e.g., for latency)
- Enhanced out-of-band signalling and synchronization
- Efficient operation.

The work will involve the identification of needed functions and their partition into functional layers. Consideration is to be given to interworking issues with present OSI conformant systems. The guidelines will take the form of a TR, entitled *Enhanced Transport Mechanism Guidelines*. [SC6 N 6887] It is in second WDTR [SC6 N 7788, December 1992].

A related NP also accepted by SC6 is on group NSAP addressing, *Enhanced Transport Mechanisms and Group NSAP Addressing* [SC6 N6892]. In a liaison statement to SC21, SC6 pointed out that at least two of the technical areas to be covered by these two new work item proposals are thought to be of particular interest to SC21 [Ref. SC21 N 6439 1991]:

- QoS enhancements
- Multipeer data transmission.

9.13.5 Multipeer Data Transmission

A May 1990 Canadian contribution to SC21 identified the basic driving forces for multipeer communications (MPC) as the coordinated interworking of more than two application processes in a single activity and use of inherently shared resources of certain subnetwork types. "Group" processing was identified as one of the next "hot topics" for standardization and was expected to include such activities as conferencing, co-authoring, sensor-based data collection, and process control—all of which involve MPC. [Ref. SC21 N 4681 1990]

Multipeer data transmission (MPDT) was originally the subject of an addendum (PDAD 2) to ISO 7498, but the work in SC21 was suspended November 1989 [SC21 N 4286]. The US national body requested reactivation of the MPDT project at the May 1991 meeting of WG1; however, the request was rejected pending technical contributions. In March 1992, the US national body requested that SC21 apply its procedures for the reactivation of MPDT [SC21 N 6197] and contributed an initial working draft text [SC21 N 6813] for an addendum to ISO 7498-1 for MPDT. The US concern was that the MPDT addendum should be the architecture that drives emerging work within the international standards community on multicast and multipeer communication, including the following [Ref. SC21 N 6812 1992]:

- ITU-TS X.6 (packet multicast service)
- ITU-TS X.gc (group communication)
- ITU-TS SGVIII multimedia (T.mcs)
- SC21/SC6, *Enhanced Communication Function in the Lower Layers*.

Also in March 1992, SC6 and ITU-TS SGVII initiated a liaison with SC21 concerning MPDT. [Ref. SC21 N 6814 1992] WG1 replied to both liaisons and stated that while it was interested in MPDT, it currently lacked the resources to pursue it. [Refs. SC21 N 7062 1992 and

SC21 N 7063 1992] Therefore, at its Plenary in Ottawa in June 1992, SC21 resolved to accept the WG1 recommendation not to reactivate the architectural work on MPDT. [Ref. SC21 N 7204 1992] However, at the 1993 SC21 Plenary, a new work item proposal, *Architecture for Multipeer Communications* [SC21 N 8003], was accepted and forwarded to JTC1. The impetus for the new effort was the need for multipeer communications for time-critical, multimedia, and ODP applications. As of July 1993, only the United States and France could commit resources to this work. In November 1993, the JTC1 reported that the new item ballot was successful, with nine nations indicating a commitment to participate (the Netherlands, Norway, and the United Kingdom declined to make such a commitment). The new work item plans a new part (WD 7498-5) to the OSI Reference Model to provide an architecture for the development of OSI services and protocols to handle multipeer communications. CD is planned for 1996, DIS in 1997, and IS in 1998. [Ref. SC21 N 8003 1993]

Among the standards progression tasks that the newly formed OSI Multipeer/Multicast (MPMC) Consortium plans to undertake are the OSI Reference Model Addendum (ISO 7498/PDAD 2) and the ANSI/ITU-TS SGVII X.PMS work. [Ref. MPMC 1991]

The ITU-TS SG VII work on multicast/multipeer covers the following aspects [Ref. SC21 N 7577 1993]:

- Development of protocols for the support by Public Data Networks of the services available to customers specified in Recommendation X.6, *Multicast Service Definition*
- Possible enhancements of the *OSI Basic Reference Model* for multicast/multipeer
- Development (or enhancement) of OSI multicast/multipeer services and protocols for various layers, including study of how the work on X.6 relates to the OSI Network Service.

A March 1993 liaison statement to SC21 from SC6/WG4 on MPDT [Ref. SC21 N 7696 1993] identifies a set of unresolved issues associated with multicast communication in the lower layers. However, current work on multicast extensions to the connectionless services and protocols of the Transport and Network layers does not depend on resolution of these issues, and should not be delayed pending their resolution. Three major unresolved multicast architecture issues are:

- Semantics of groups and group membership
- Specification of the phases of operation for multicast communication
- Way in which information about multicast conversations is exchanged ("data flows").

In addition, the liaison statement identifies the following unresolved issues that are specific to the transport layer: semantics of join, semantics of multicast data transfer, reliability, sequencing, semantics of multiple leaves and joins, and scope of multicast transport.

Multipeer data transmission has been identified as essential to time critical communications (see Section 9.13.6). ISO/TC184 SC5/WG2 identified this need in TR 12178, *User Requirements for Time Critical Communications,* and in a December 1993 liaison statement to SC21 [SC21 N 8384]. Reliance only on peer-to-peer communications is seen as too limiting for the following reasons: temporal consistency of replies to requests from two peer entities for the same service at the same time, and spatial coherence for a request from a peer entity for several entities to provide simultaneously a service or services. SC5/WG2 has developed a multi-peer model, *Produce, Distributor, and Multi-Consumer Model,* to ensure data can be distributed to a number of peer entities. [Ref. SC21 N 8384 1993]

At its June/July 1993 meeting, Study Group 7 of ITU-TS reaffirmed its intention to develop an architecture for OSI multicast data transfer, covering all seven of the OSI layers, which will be compatible with ITU-TS X.6 and with other ongoing work within the ITU-T concerning efficiency of OSI protocols, multicast, and multimedia communications. Because of its commercial importance, multicast data transfer will be progressed in SG7 with high priority. SG7 has offered a joint editor if SC21 responds favorably to the October 1993 ITU-TS invitation to jointly produce a common test format for this architectural enhancement to the OSI Reference Model. [Ref. SC21 N 8267 1993]

9.13.6 Time Critical Communications (TCC)

As noted in Section 9.13.5, TC184 SC5/WG2 is developing standards for time critical communications (TCC). A liaison statement from SC21 [SC21 N 7065] in May 1992 proposed a partition of elements of work among various groups, with SC21 acting as the bridge for groups in JTC1 working on time critical communications. In order to gain formal approval to begin work on architecture, SC21/WG1 circulated Question 1/65 within SC21, which was approved in May 1992 at the SC21 plenary. SC21/WG1 is working on the Time Critical Communications Architecture (TCCA).

In December 1993, TC184 SC5 forwarded the IS text of TR 12178, *User Requirements for Systems Supporting Time-Critical Communications*, to ISO for publication. TR 12178 addresses the need for performance and resilience for time critical communications, especially when time-critical and non-time-critical traffic coexist, and specifies requirements for a TCCA. The focus is identification of communications needs of tightly coupled control systems. The work is intended to complement efforts focused on factory information networks [e.g., Manufacturing Automation Protocol (MAP); see Section 9.11.5.1], which are characterized by high throughput, large packet service between information process and control processors. The effort is also intended to identify sensor networks (e.g., fieldbus) that concentrate on providing low complexity interface to simple factory floor sensors, actuators, and other devices. [Ref. SC21 N 8385 1993]

9.13.7 Minimal OSI Upper Layers and Skinny Stacks[56]

A full OSI stack provides most, possibly all, facilities and options in a set of standards (e.g., in the upper layers). A skinny (upper layer) stack (sometimes called a thin stack) provides protocol facilities that exactly match the requirements of the supported applications, in a fully OSI conformant way. A stack is termed "fat" if it provides protocol facilities that (far) exceed the requirements of the supported applications. A short stack has no upper layers—the applications are on top of the Transport Layer.

ISO/IEC ISP 11183, *Common Upper Layer Requirements*, defines a Minimal OSI (mOSI), which is a subset of full upper layer protocols that exactly matches the requirements of a basic connection-oriented application (BCA—which itself only requires connect/disconnect and send/receive services—thereby providing skinny facilities). BCAs typically use only 5 percent of the functionality of a full stack, but most OSI platform implementations are full OSI stacks, implying that for most applications the full implementation products are fat. The unused code can be expensive in terms of investment, storage, and execution.

[56] This section is based on the November 1993 briefing to EWOS: [EWOS/TA/93/399].

Facilities of mOSI include a kernel functional unit at each layer with optional functional units, such as authentication and application context name negotiation in the Application Layer. One or more presentation contexts are provided in the Presentation Layer, and two-way simultaneous functional unit and 512-octet user data for S-CONNECT in the Session Layer.

Potential applications of mOSI are in the Industry/Government Open Systems Specification (IGOSS) (see Section 16.1.3.3), X/Open's XTI, thinOSI, being addressed by the IETF for Internet, and thinOSI prototypes, such as one developed at the University of Florida. Evaluations of performance are ongoing.

9.13.8 TCP/IP-OSI Convergence and Coexistence[57]

As noted in Sections 9.7.4 on Internet Standards above, in profile discussions in Chapter 16, and in discussions of NATO and national CCIS initiatives in Chapters 18 and 19, the continued use of TCP/IP in conjunction with transition to OSI is a major issue for the nations and the national bodies participating in international standardization. Many existing and emerging information systems, including CCISs, have both Internet and OSI standard services and protocols. Multinational recommendations for GOSIPs (e.g., IGOSS, see Section 16.1.3.3) do this as well. Version 3 of the US Application Portability Profile and US GOSIP await decisions from policy makers and standards experts on the convergence and coexistence of TCP/IP and OSI. (See Section 16.1.8.)

One initiative in this area is establishing formal liaison between the Internet Society (ISOC)/Internet Architecture Board (IAB) and ISO/IEC JTC1/SC6. SC6 has proposed C-liaison status; the Internet Society requested A-liaison status with JTC1. Unofficial liaison in the form of attendance at meetings has been ongoing for some time. Areas of common interest are use of CLNP to ameliorate the problem of inadequate address space for the Internet Protocol Suite and common interest in ECFF (see Section 9.13.3) to support multimedia and hypermedia applications.

EWOS/TA held a special meeting in October 1993 on TCP/IP-OSI convergence, with focus on the future relationship between OSI and TCP/IP and the potential role of EWOS in the emergence of this relationship. The key requirements of users are for a global lower-layer service with a well-defined API that supports ISDN and ATM, optionally selectable according to user needs, and for a multiplicity of applications that fulfill a range of functional requirements. A further requirement is for the protection of existing investment. OSI and TCP each represents a solution for these requirements. Options for achieving a single solution may rely on Government edict (not wholly successful), market forces (which might lead to chaos), and active definition of either an entirely new solution or one that permits the coexistence of both in a way that allows the aforementioned requirements to be fulfilled.

Limitations on the selection and specification of a solution to the convergence issue include existing mandates on GOSIP, EEC and national rules on choices available to public procurers; parallel use of OSI connection-mode and connectionless-mode services; and the fact of ongoing development and enhancement of products and protocols by both OSI and Internet communities. For the long term, there may be a requirement for a new "base" networking standard for the lower layers. Possible short-term options are the following:

- New relay and transport profiles for TCP/IP
- Minimal OSI (mOSI), aimed at making OSI more competitive

[57] This section is based on the October 1993 EWOS report of a special session of EWOS/TA [EWOS/TA/93/391].

- Application converters
- Lower layer profiles offering an API platform for applications.

The October 1993 EWOS meeting conducted separate discussions on the lower layers and the upper layers concerning the requirements and needs for standardization for four approaches. These approaches are defined as follows:

- Coexistence—several protocol architectures running on the same physical network, each providing different network services and each with its own API. The networks are essentially isolated with any bridging between applications on the different networks achieved through Application Layer gateways rather than the Network/Transport Layer.
- Interoperability—involves bridging or relaying at the Network or Transport Layer to provide one, seamless network service with a single address space.
- Convergence Protocol and API—a single protocol and a single API at the Network/Transport Layer.
- Convergence API only—a single API at the Network/Transport Layer with many underlying protocols. This aids in portability of applications.

One outcome of the October 1993 meeting was a new work item proposal on ISO/Internet Management Coexistence Process. This will focus on the need for integrated management of many different components that may be accessed by ISO/ITU-TS management and Internet management. Of particular interest is the management of Internet SNMP agents by ISO/ITU-TS CMIP managers, taking advantage of the numerous SNMP management information bases (MIBs). The technical report produced would contain a description of the coexistence strategy based on the use of translated MIBs in either a proxy or native implementation. [Ref. EWOS/TA/93/355 1993]

9.14 Assessment of Coverage by Standards

Network services can be provided for CCISs using OSI protocols for electronic mail, Directory, file management, and exchange of telematic information and documents. At the present time, there are not many high-level services provided by the OSI stacks, but the communications aspects at lower layers are mature for connection-oriented services and maturing rapidly for connectionless-mode services. Only proprietary products are now available with ISDN services and protocols, and ISDN usage is not yet widespread in the United States. IEEE has developed a draft standard (P1003.8 Draft 6) for Transparent File Access (TFA). TFA-like features are available in several products, but there is as yet no common specification for such file system semantics.

Analysis is now being performed in TSGCE SG9 to identify additional features required for military application of MHS (see Section 17.3.4.2). Analysis of the relationship of MHS to ACP 129 and ASN.1 to STANAG 5500 and other message standards is needed. NATO has requirements for media independent data communications protocols (e.g., for Link 1 replacement) that have not yet been developed; these standards could be applicable to the communications services, and more work needs to be done in this area (see Section 17.5.1).

In a comparison of the 65 service elements of ACP 127, an analysis [Ref. USPR 1989] has identified 55 as common to MHS-88. An additional five service elements were shown to be related to, but not the same as, those in ACP 127:

- Precedence levels (MHS-88 provides an Importance Indicator)
- Message identification (MHS-88 provides somewhat different features)

- Prosign C (MHS-88 has an obsoleting indication)
- Bell signal (MHS-88 provides a stored message alert)
- Date-time group (MHS-88 has a submission time stamp).

Five services provided in ACP 127 are not supported in MHS-88: financial accountability, service message, network continuity indication, off-line accountability, and tracer action.

10. OPERATING SYSTEM SERVICE STANDARDS

10.1 Requirements

Operating system services allow applications to gain access to system resources in terms of task initiation, management, scheduling, resource allocation, logical and physical device access, interrupt handling, communication, synchronization, accounting, file management, and a range of utilities that assist efficient development, testing, and execution of applications software. Operating system services address kernel services, commands and utilities, system administration and management, and security. An overview of standards for operating system interfaces is given in Table 31.

10.2 Standards for Operating System Services

The key enabler for standardizing operating system services is the use of a robust standard for the operating system *interfaces*. If the interface standard is sufficiently robust (providing a wide range of services), then adherence to the standard can provide the needed functionality without having to be limited on choice of an operating system and thereby an operating environment. Many implementations available today provide the basic operating system interface. Use of options for additional services outside a standard interface could defeat the goal of adopting a standard interface for operating system services, namely ensuring a high degree of applications portability while providing the necessary system services for information exchange and applications.

10.2.1 POSIX

The Portable Operating System Interface for Computer Environments (POSIX) is an interface standard for operating systems that is designed to be vendor independent and to promote application portability. In ISO it is being developed as ISO 9945.

Table 31. Status Overview of Key Operating System Interface Standards

	LOC	PAV	CMP	MAT	STB	DFU	PRL
FIPS 151-2 POSIX	●	●	●	●	●	●	●
IEEE 1003.2 POSIX Shell	○	●	●	●	●	●	●
IEEE P1003.4 Realtime	○		○	●	○		
IEEE P1003.1e, 2c Security				○			

LOC – Level of consensus
PAV – Product availability
CMP – Completeness
MAT – Maturity
STB – Stability
DFU – De facto usage
PRL – Problems/limitations

Key: ● High Evaluation
○ Average Evaluation
Blank Low Evaluation

Source: [Ref. APP 1993]

10.2.1.1 POSIX Development

Development of the POSIX standards is through the Institute of Electrical and Electronics Engineers (IEEE) Computer Society's Portable Application Standards Committee (PASC) [formerly the Technical Committee on Operating Systems (TCOS)]. [Ref. CFS 1993b] The PASC has formed a large number of working groups. These working groups and the POSIX standards being developed were identified by the same label, namely P1003 with an appropriate extension. However, this numbering system was revised in September 1993 to reflect changes in relationships among the standards. Of these, IEEE 1003.1, IEEE 1003.2, IEEE 1003.2a, IEEE 2003 (formerly IEEE 1003.3), IEEE 1003.1b (formerly IEEE 1003.4), IEEE 1003.5, IEEE 1003.9 and IEEE 1224.2 (formerly IEEE 1003.17) have achieved standards status. The scope and status of the POSIX work in IEEE is provided in Table 32.

POSIX base standards include IEEE 1003.1, IEEE 1003.2, and IEEE 1387. The following are amendments to IEEE 1003.1: IEEE 1003.1c (*Threads Extensions*), IEEE 1003.1e (*Security Extensions*), IEEE 1003.1f (*Transparent File Access*), IEEE 1003.1g (*Protocol Independent Interfaces*), IEEE 1003.15 (*Batch Extensions*). Current POSIX profiling projects include: IEEE 1003.10 (*Supercomputing Profile*), IEEE 1003.13 (*Real-Time Profiles*), IEEE 1003.14 (*Multi-processor Profile*), and IEEE 1003.18 (*Platform Environment Profile*). The Transaction Processing Profile Working Group (IEEE 1003.11) recently disbanded [Ref. OSN 1993h], and the project has been withdrawn.

Table 33 summarizes the status of POSIX and POSIX-related standards being developed by IEEE (see Table 32 for details).

NIST's FIPS 151-1 was based on the 1988 version of IEEE 1003.1. The revision completed in 1990, FIPS 151-2, aligns it with IEEE 1003.1-1990.

WG15 of SC22 within the JTC1 was formed in September 1987 and assigned responsibility adopting IEEE POSIX standards as international standards. The IEEE standard P1003.1 was adopted as ISO 9945-1 in 1990. SC22/WG15 eventually intends to remove the focus on UNIX and the C language to create a generic interface specification between any language and a multiuser environment. WG15 has formed four rapporteur (expert) groups: Conformance Testing, Internationalization, Security, and Coordination of Profile Activities. WG15's division of work items is as follows:

- ISO 9945-1, *System Interface*, 1990
- CD 9945-1.1, *Language Independent Base* (P1372)
- CD 9945-1.2, *Real Time and Extensions* (P1003.1b)
- CD 9945-1.3, *Distribution Services* (P1003.1f)
  - CD 9945-1.3.1, *Transparent File Access* (P1003.1f)
  - CD 9945-1.3.2, *Remote Procedure Call* (P1237)
  - CD 9945-1.3.3, *Transport Interface*
  - CD 9945-1.3.4, *Name Space/Directory Services* (P1003.1g)
- DIS 9945-2.1, *Shell and Utilities* (P1003.2)
- CD 9945-2.2, *User Portability Extensions* (P1003.2a)
- CD 9945-3, *System Management* (P1387)
- CD 9945-3.1, *General Services* (P1387)
- CD 9945-3.2, *Batch Services* (P1003.15).

Table 32. POSIX Standards Being Developed by the IEEE for Submission to ISO Through ANSI

P1003.0, *POSIX Guide*—accelerates consensus on Open Systems for Applications Portability and provides timely guidance to users on how to develop applications profiles. It contains the POSIX Open System Environment (OSE) Reference Model (Draft 15, July 1992)

1003.1, *POSIX*—Standard operating system interface and environment to support application portability at the source code level. Approved (IEEE Std. 1003.1-1988) revised September 1990 (IEEE Std. 1003.1-1990). ISO 9945-1: 1990. FIPS 151-1 was equivalent to IEEE Std. 1003.1-1988. FIPS 151-2 is same as 1990 version

P1003.1/LIS, see IEEE P1372

P1003.1a, *System Interface Extensions*—additional functions, preparatory work for Language Independent Specifications. (Draft 7, 3Q, 1993)

1003.1b, *Real-Time Extensions*, approved October 1993 (formerly IEEE P1003.4)

P1003.1c, Amendment to POSIX.1: *Threads*—defines interfaces for handling multiple threads of control within a single POSIX process. (Draft 8 recirculated May 1993) (formerly IEEE P1003.4a)

P1003.1d, Amendment to POSIX.1: *Extensions to .4*—extend interfaces defined by POSIX.1 and POSIX.4 to include additional real-time facilities. (Draft 4, September 1992) (formerly IEEE P1003.4b)

P1003.1e, *Protection, Audit and Control Interfaces [C Language]* (formerly IEEE P1003.6.1)

P1003.1f, *Transparent File Access (TFA)*—develops system interfaces and other mechanisms to permit portability of applications into environments where files, directories, etc., may reside on remote systems. (Draft 6, April 1992, recirculated November 1992) (formerly IEEE P1003.8)

P1003.1g, *Protocol Independent Interfaces*—defines programmatic interfaces that allow a portable application to communicate with another entity in the network such that the application may be independent of the underlying protocols. (Draft 1, September 1992) (formerly IEEE P1003.12)

1003.2, *Shell and Tools*—defines a standard source-code-level interface to shell services and common utility programs for applications programs. (Draft 12 approved September 1992) (DIS 9945-2: 1992). Currently in the FIPS adoption process. NIST expected to adopt 1003.2 as a FIPS by December 1993.

1003.2a, *User Portability Extension*—provides extensions...to support terminal users in a consistent manner across all conforming systems. Approved as part of 1003.2, September 1992.

P1003.2b, Utilities *Extensions*

P1003.2c, *Protection and Control Utilities* (formerly IEEE P1003.6.2)

1003.3, see IEEE 2003

1003.3.1, see IEEE 2003.1

P1003.3.2, see IEEE 2003.2

P1003.4, see IEEE 1003.1b

P1003.4a, see IEEE P1003.1c

P1003.4b, see IEEE P1003.1d

1003.5, *POSIX Ada Binding*—determines the Ada environment interface and Ada extensions required for POSIX; provides a specification for the Ada environment interfaces and Ada required extensions so that applications programs can be written to operate consistently on all conforming POSIX/ Ada environments. (Approved June 1992) A PAR for a revision to this standard was approved October 1993. The new title will be *POSIX Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API).*

P1003.5b, *Ada Language (Real Time) Bindings*—develop an Ada language binding to the real time POSIX standards. Expected to start balloting December 1993 (formerly IEEE P1003.20)

P1003.6, see IEEE P1003.1e and see IEEE P1003.2c

P1003.6.1, see IEEE P1003.1e

P1003.6.2, see IEEE P1003.2c

P1003.7, see IEEE P1387

P1003.7.1, see IEEE P1387.4

P1003.7.2, see IEEE P1387.2

P1003.7.3, see IEEE P1387.3

P1003.8, see IEEE P 1003.1f

1003.9, *POSIX FORTRAN 77 Binding*—defines a FORTRAN-1977 language binding to applicable POSIX interfaces and functionality as specified in P1003.1,2,4, etc., and establishes an interface for FORTRAN to POSIX such that FORTRAN applications using POSIX functionality will be portable at the source code level. (Draft 11 approved June 1992)

P1003.10, *Supercomputing Application Environment Profile (AEP)*—develops an AEP for supercomputing environments. (Draft 11, September 1992)

Table 32. (Cont'd)

P1003.11, *Transaction Processing AEP*—develops a standard profile for transaction processing application environments. (Draft 7, July 1992) Working Group recently disbanded. WITHDRAWN
P1003.12, see IEEE P1003.1g
P1003.13, *Real-Time AEP*—defines an AEP for real-time applications using the POSIX interfaces; addresses three profiles: full-function real-time system, embedded control system, and intermediate real-time system. (Draft 5, May 1992)
P1003.14, *Multiprocessing AEP*—defines an AEP for multiprocessing applications environments based on relevant POSIX standards. (Draft 7, April 1992)
P1003.15, Amendment to POSIX.1: *Batch Environment Amendments*—define utilities, library routines, system administration interfaces, and a host-to-host protocol to provide a network queueing and batch system in a POSIX environment. (Draft 12, December 1992)
P1003.16, C *Binding for POSIX.1*—defines a C-language binding between ISO/IEC 9945.1:199x and the C standard. (Draft 12, December 1992) [PAR WITHDRAWN OCTOBER 1993]
P1003.16a, *Amendment 1: System API Extensions* [PAR approved, March 19, 1992] [PAR WITHDRAWN OCTOBER 1993]
1003.17, see IEEE 1224.2
P1003.18, *POSIX Platform Profile*—establish a Platform Environment Profile based on the ISO 9945 work and related standards that describes a simple foundation for an interactive, multiuser application platform. (IEEE standard is under balloting)
P1003.19, *FORTRAN 90 Language Bindings*—develop FORTRAN 90 language binding to the Language Independent Specification of the POSIX system application program interface upon approval of the project by the IEEE Standards Board. Initiated July 1992. [PAR WITHDRAWN OCTOBER 1993]
P1003.20, see IEEE P1003.5b
P1003.21, *Real-Time Distributed Systems Communication (RTDSC)* —develop an application interface standard that meets the needs of the distributed real-time mission-critical computing domain. Expected to start IEEE balloting in July 1995.
P1003.22, *Guide to the POSIX Open Systems Environment - A Security Framework*
1224.2, *Directory Services API*—defines an application programming interface to a directory service, X.500 functionality. Approved March 1993 (formerly IEEE P1003.17)
P1372, *Language Independent Specifications (LIS)*—to provide a computer language independent specification that corresponds exactly with IEEE Std. 1003.1-1990. (Draft 16, 2Q 1993) Target completion 4Q1993 (formerly IEEE P1003.1/LIS)
P1387, *Administered Systems (name changed from System Administration Interface)*—defines a standard interface to utility programs for administering systems that conform to POSIX. Work is being "sliced" into ballotable partitions. (formerly IEEE P1003.7)
P1387.2, *Software*, (Draft 8, March 1993) (formerly IEEE P1003.7.2)
P1387.3, *User Administration*, (PAR approved October 1993) (formerly IEEE P1003.7.3)
P1387.4, *Printing*, (Draft 7, June 1993) (formerly IEEE P1003.7.1)
P2003, *Test Methods: General*—defines general requirements and test methods for test suites to measure conformance of an implementation to IEEE POSIX and related standards. Approved March 1991 (IEEE Std. 1003.3-1991) ISO CD ballot initiation (formerly IEEE P1003.3)
P2003.1, *Test Methods for POSIX.1*—defines test methods and test assertions for POSIX Approved December 1992. ISO NP ballot closed January 1993 (formerly IEEE P1003.3.1)
P2003.2, *Test Methods for POSIX.2*—defines test methods and requirements for implementations of test suites to measure conformance to POSIX.2. (Draft 8, July 1992) (formerly IEEE P1003.3.2)

Source: "Applications Portability and Open Systems Environments: Status Report," Roger J. Martin, NIST, presented at the *11th APP/OSE Workshop*, NIST, Gaithersburg, Maryland, May 1993. Updated periodically from *IEEE Standards Bearer* and *Open Systems Standards Tracking Report*

Part 3, *Test Methods (General)*, was approved as IEEE standard 1003.3-1991 on March 1991, but is now redesignated as IEEE 2003. IEEE P1003.3.1, *Test Methods for POSIX.1* was approved December 1992 and has been redesignated IEEE 2003.1. Part 5, *Ada Bindings* was approved June 1992. Part 9, *FORTRAN 77 Bindings* was approved as an IEEE Standard in July 1992.

Table 33. Status of POSIX Standards

POSIX Standard	Title	Status	Likely Date of Standard Approval
P1003.0	POSIX Guide (OSE Reference Model)	Draft	Late 1994
1003.1	POSIX System Interfaces	Approved	FIPS 151-1
P1003.1a	POSIX System Interface Extensions	Draft	1994
P1003.1b	Real-Time Extensions	Draft	1994
P1003.1c	Threads	Draft	TBD
P1003.1d	Extensions to P1003.1b (LIS)	Draft	TBD
P1003.1e	Security Interface	Draft	1994
P1003.1f	Transparent File Access	Draft	1994
P1003.1g	Protocol Independent Interfaces	Draft	1994
1003.2	Shell and Utilities	Approved	Sep 1992
1003.2a	User Portability Extensions	Approved	Sep 1992
P1003.2b	Utilities Extensions	Draft	1994
P1003.2c	Security Interface	Draft	1994
1003.3.1	Test Methods for POSIX.1	Approved	Dec 1992
1003.3.2	Test Methods for POSIX.2	Draft	TBD
1003.5	Ada Bindings	Approved	June 1992
P1003.5b	Ada Real-Time Binding	Draft	1994
1003.9	FORTRAN Bindings	Approved	June 1992
P1003.10	Supercomputing AEP	Draft	1994
P1003.11	Transaction Processing AEP	Draft	Withdrawn
P1003.13	Realtime AEP	Draft	1994
P1003.14	Multiprocessing AEP	Draft	Early 1994
P1003.15	Batch Environment Extensions	Draft	Early 1994
P1003.16	C Bindings	Draft	Withdrawn
1003.17	Directory Services/Name Space	Approved	March 1993
P1003.18	POSIX Platform Profile	Draft	1994
P1003.19	FORTRAN-90 Binding	Draft	Withdrawn
P1201.1	User I/F (Interfaces)	Draft	TBD
P1201.2	User I/F (Driveability)	Draft	1994
1224.1	X.400 E-MAIL API	Approved	March 1993
1224.2	Directory Services/Name Space	Approved	March 1993
P1238	OSI Connection API	Draft	1994
P1238.1	OSI FTAM API	Draft	1994
P1372	Language Independent Spec. (LIS)	Draft	TBD
P1387	Administration	Draft	Early 1994
2003	General Test Methods	Approved	March 1991
2003.1	Test Methods for POSIX.1	Approved	December 1992
2003.2	Test Methods for POSIX.2	Draft	1994

Source: *Technical Reference Model for Information Management*, Version 2.0, Coordination Draft, Center for Information Management, DISA, 22 June 1993; *Open Systems Standards Tracking Report*, Volume 3, Number 1, January 1994, p. 3; and [Schoka 1994].

POSIX is intended to be compatible with both Database Language SQL and IRDS database management languages, as well as with OSI data communications and interprocess communications.

IEEE POSIX Security Working Group (formerly P1003.6) is defining security extensions to the base POSIX interface standard (ISO 9945-1), to include support for audit, privilege, discretionary and mandatory access control, and information labels. These have been redesignated IEEE P1003.1e and IEEE P1003.2c.

IEEE P1372, POSIX, Part 1: *System Application Program Interface (API)* [Language Independent] is a new POSIX effort. It was formerly designated IEEE P1003.1/Language Independent Specification (LIS).

The System Management FIPS, the GOSIP Network Management (GNMP; FIPS 179) was issued 14 December 1992. Planned FIPS based on the POSIX standards include a Transparent File Access (TFA) FIPS based on P1003.1f and a System Management FIPS based on P1387. Plans were to make the initial FIPS proposal for the Transparent File Access FIPS in early 1993 with the expectation that a FIPS would be approved by early 1994.

10.2.1.2 POSIX Conformance Testing

IEEE Std. 2003.1-1992, *IEEE Standard for Information Technology—Test Methods for Measuring Conformance to POSIX - Part 1: System Interfaces*, defines conformance test methods for the POSIX.1 standard, based on the methodologies outlined in IEEE 1003.3.

The NIST Computer Systems Laboratory (NCSL) has developed a POSIX Conformance Test Suite (PCTS) based on IEEE 1003.1-1988 (FIPS 151-1). The suite was in beta testing for over a year and is available from the National Technical Information Service (NTIS). The NIST National Voluntary Laboratory Accreditation Program (NVLAP) will accredit testing laboratories that will be referred to as Accredited POSIX Testing Laboratories (APTLs). On May 1991, NVLAP announced the initial group of seven labs. The policy document for POSIX Conformance Testing is *NVLAP Program Handbook Computer Applications Testing - POSIX Conformance Testing*. Testing is done through agreement between the testing lab and the client, without NIST/CSL involvement. However, NIST/CSL issues the certificate of validation. [Ref. Hall 1991]

An updated FIPS (FIPS 151-2) points to the 1990 version of the base standard (IEEE 1003.1-1990), and updates certain limits based on experience. A new test suite is being provided that very closely matches the methods described in IEEE 2003.1-1992. [Ref. OSN 1993h]

The Conformance Testing Service has established a CTS-2 POSIX Project with the goal of a harmonized European and internationally recognized conformance testing service for POSIX. Participants in the project include the National Computing Centre Ltd (UK), the Computer Resources International A/S (Denmark), X/Open Company Ltd (UK), and British Telecommunications (UK). The project will be establishing test laboratories throughout Europe and seeking cross recognition with NIST. [Ref. Pink 1991]

10.2.2 Consortia Recommendations

Standards activities in areas related to the operating systems have been primarily in the area of developing international, nonproprietary standards for *interfaces* to operating systems. It appears unlikely that an international standard for an operating *system* will be developed, in part because operating systems are closely tied to the hardware architecture of vendor products.

As indicated earlier, POSIX is becoming a widely accepted approach to standardizing interfaces to operating systems; the initial standard for POSIX (ISO 9945-1) has been completed. Consortia have been formed to develop and promote profiles of standards that could be the basis for open environments and portable systems within these environments. All the consortia have adopted POSIX; however, there are differences in the approaches being taken. Activities of these consortia in the POSIX area are discussed in this section; additional information on portability profiles is provided in Chapter 15.

X/Open. The international nonprofit consortium X/Open developed extensions to UNIX System V Interface Definition (SVID), which define a distributed (two-phase) transaction processing environment that meets OSI standards. A layered functional model for this environment that consists of resource, commit, and transaction management has been proposed. This model requires certain extensions to the UNIX kernel (guaranteed output to files and concurrent input from peripherals). The X/Open System V Specification (XVS) is the initial recommended standard for the operating system. The extensions would be part of a Common Applications Environment (CAE), a concept to promote software portability. This would be achieved by adopting and adapting existing industry and de facto standards, rather than by creating a new standard. Future goals for the CAE are alignment[58] with POSIX P1003.1 (with a large number of extensions) and ANSI X3J11 C together with interfaces for Indexed Sequential Access Method (ISAM) and an embedded standard relational database language (SQL). The X/Open version of ISAM is based on a major (implementation nonspecific) subset of C-ISAM Version 2.10 (January 1985) from the Informix Corporation. The initial X/Open version of SQL is not fully compliant with ANSI X3.135-1986 [Ref. X/Open 1987; X/Open 1988; Lambert 1987]. Standards recommended for the CAE are discussed in Section 15.1.3.4. X/Open now has an agreement to acquire the UNIX trademark (see Section 10.2.3).

OSF. Another approach to developing standard interfaces to UNIX-type systems is being taken by the OSF, an international consortium formed in May 1988. OSF's operating system, OSF/1 was initially based on the IBM AIX, a version of USL's System 5, Release 3.2. Release 1.0 became available for general release in November 1990, Release 1.1 in June 1992, and Release 1.2 in June 1993. It is XPG4 and POSIX 1003.2 compliant. General availability of Release 1.3 is scheduled for second quarter 1994. Release 1.2 is based on Mach 2.5. Release 1.3 will be based on Mach 3.0 and derived from the OSF Research Institute's MK5 operating system version. As of March 1993, 10 companies had announced ports to 12 machine architectures. Sections 15.1.2.4 and 15.1.3.5 discuss OSF.

OSF/1 is based on Version 2.5 of a microkernel operating system called Mach that was developed at Carnegie Mellon University (CMU) under the direction of Rick Rashid (now Director of Research at Microsoft Corporation). The microkernel is used to provide a virtual platform on which an operating system may be based. Services provided include process-to-process communication, threads of control, and mapping of virtual memory to physical memory.

The OSF Research Institute is working on a new version of the Mach kernel that is derived from Version 3.0 of the CMU effort. The new microkernel adds support for symmetric multiprocessing and C2-level security. This version will become part of OSF/1 and part of the IBM's Workplace OS that will run on PowerPC and Intel platforms.

COSE. One of the most interesting developments is the formation of an alliance between three UNIX system suppliers (Sun, HP, and IBM) and three software suppliers (USL, SCO, and Univel) to support a specification known as the Common Open Systems Environment (COSE). The COSE specification is designed to provide a common desktop environment for UNIX, together with agreed standards for networking and management. [Ref. RNLA 1994, p. 30] Its first output is a white paper on *Open System Process Acceleration* (June 1993). The white paper states that the intent of COSE is to accelerate the process by which open system software

---

[58] The October 1992 version (XPG4) of the *X/Open Portability Guide* is aligned with POSIX.

specifications are defined and submitted to recognized industry standards forums. [Ref. OSN 1993n]

10.2.3 Operating System Standards

OSCRL. In the 1980s, SC21/WG8 began work in the area of Operating Systems Command and Response Language (OSCRL). A draft proposal for OSCRL was planned but never promulgated. The project is currently inactive.

UNIX SVR4. UNIX System V Release 4 (SVR4) represents an attempt to incorporate the best technology from the most popular versions of UNIX (System V, SunOS, and Xenix), offering extensive levels of compatibility, portability, and interoperability. New features designed into SVR4 include support for the following: multiprocessing, multilevel security, greater reliability, enhanced system administration, POSIX compliance, improved scheduling and real-time processing, DCE and COBRA support, multinational language support for all major European languages as well as Japanese, future support for OSF's Distributed Management Environment (DME), and use of CHORUS (Section 5.2.11) microkernel technology. OSF/1 represents an alternative to SVR4, using a Mach kernel with UNIX functionality that is based on Berkeley 4.4. Features of OSF/1 include the following: sophisticated support for threads and parallelism (based on Mach), POSIX-compliance, support for multiple file systems [including Sun's Network File System (NSF)], dynamic configuration, shared libraries, advanced security features (compliant with C2 rating in the Orange Book), and extensive internationalization (locale databases in most major European languages, as well as multinational language support). [Ref. RNLA 1994, pp. 43-44]

Mach. An alternative multi-processor operating system to UNIX is the Mach operating system developed by the Carnegie Mellon University with DoD funding and designed to control one to tens of processors. Mach is compatible with the Berkeley variant of UNIX and has been ported to a number of platforms. Although Mach is not a commercial product, it conforms to the IEEE POSIX standard and forms the core part of OSF's OSF/1 operating system. [Ref. RNLA 1994, p. 31]

UNIX International. UNIX International (UI) (formerly Archer, with a membership of 42 corporations and user groups) promotes UNIX System V, formerly a proprietary standard of AT&T. Release 4.2 of UNIX System V is now available.

During 1991, the UI membership requested that UI expand its scope and begin addressing a complete systems software environment for open systems. As a result, UI has defined UI-ATLAS (see Section 15.1.3.9). The 1993 UI Roadmap calls for the delivery of 20 new technology components and defines requirements for improved interoperability with existing systems and enhanced support for multimedia standards in future UNIX System versions. Technology candidates include: object-oriented management, Windows emulation, and federated naming. UI has widened the development process to take input from suppliers outside of UNIX Systems Laboratories (USL), setting up a process similar to OSF's requests for technology (RFTs). SunSoft's ONC+ is the first non-USL Reference technology. X/Open's role in managing the common UNIX API (see Section 15.1.3.4) will take over a large part of UI's role in creating a roadmap for UNIX, although UI's roadmap extends beyond the operating system, including distributed computing and management. [Ref. OSN 1993q]

In June 1993, UI issued its first RFTs for technology that will enable users to link objects between documents created by different UNIX applications. The technology will allow users to

incorporate data such as graphics, created in one software package, into a separate application, into a separate application, on the same desktop, or across a network. It must be compatible with and complementary to the COSE environment and must comply with OMG's CORBA. UI expects that the technology will be widely deployed in the first half of 1994. [Ref. OSN 1993i]

In December 1992, Novell announced its purchase of UNIX Systems Laboratories. Then, in October 1993, Novell and X/Open announced an agreement that would confer Novell's "UNIX" trademark to X/Open. The proposed agreement would allow X/Open to certify industry-standard UNIX operating systems based on a common set of X/Open application programming interfaces (APIs) (see Section 15.1.3.4). The unified UNIX will be built on X/Open's Spec 1170, a common set of 1,170 APIs that vendors can enhance in their own UNIX implementations. The UNIX API (as the 1170 Spec is now called) will end the necessity for suppliers to adapt their code to different features of various UNIX flavors and will cause the UNIX market to settle down to a small number of implementations, but not to reduce to a single version. The move is expected to give the UNIX world a united front against other 32-bit operating systems such as Microsoft's Windows NT and IBM's OS/2. [Ref. OSN 1993q; OSN 1993r] Novell will continue to sell its UNIX System Group's System V operating system source code, likely under the name of UNIX-Ware, which is a Novell-specific implementation of the Spec 1170 APIs. [Ref. Bozman 1993; Maggelet 1994]

Microsoft hopes that its NT operating system will lock UNIX out of any majority share of business desktops. [Ref. OSN 1993] In December 1992, UI released an independent report that predicts that Microsoft NT will become a dominant desktop operating system, but will not displace UNIX from the server market. [Ref. OSN 1993d] A June 1993 article [Ref. OSN 1993l] claims that as Microsoft announces and delivers its long-heralded NT operating system, support is spreading among system vendors. In addition to Digital Equipment that has long supported it, Hewlett Packard and NCR have also moved to support it.

10.2.4 Microkernel Architectures

Operating systems developers are moving, en masse, from integrated monolithic architectures to microkernel architectures. The microkernel architecture approach provides for the separation of operating system functions into a core, which will run in the most privileged state of the computer, and the rest, which run as a set of applications in nonprivileged or user space. The two parts then interact via a clearly defined set of interfaces. This results in systems that are more secure, more robust, and easier to maintain, extend, and scale. Both the next generation of UNIX releases from USL due for release in 1994 (based on CHORUS System's microkernel technology) and the next OSF operating system (planned for release as OSF/1.3 MK in 1994 and based on the Mach 3 architecture from CMU) will have microkernel architectures. [Ref. RNLA 1994, p. 31; Goulde 1993]

Microkernel architectures use message-passing communications between the kernel and the user-space servers, which can be used in multiprocessing architectures, clustered configurations, and massively parallel architectures. These architectures permit operating system upgrades without having to bring down an information system during installation and tend to recover faster than monolithic kernels because of their reduced complexity. [Ref. Goulde 1993]

10.3 Assessment of Coverage by Standards

Operating system services include kernel operations, commands and utilities, system management, real-time extensions, and security. Four of these areas (management is excluded) are addressed by POSIX. The POSIX standard provides the broadest applicable reference model for developing portable applications at the source code level. Considerable progress has been achieved, and there is still additional work in process. [Ref. OSN 1993h]

Standardization of operating systems appears unlikely. Further, there is no need to select a standard operating system for an automated information system, since such a selection is viewed as an implementation issue. When mature, adopting the POSIX interface standard for information systems appears to be an attractive option, both to achieve some of the required system services and to promote applications portability during implementation. Adoption of the current POSIX standard would probably not fully meet system service requirements. For example, POSIX addresses independent operating systems cooperating in a distributed environment, not a single operating system running on multiple machines. It is not specifically designed for distributed applications, and therefore may not serve an information system's needs completely.

Moreover, IEEE 1003.1-1988, *System Application Program Interface* (FIPS 151-1 and ISO 9945-1) does not include the capabilities for kernel security that are typically provided in an operating system kernel. Also required are real-time profiles (IEEE P1003.13) and testing specifications.

Recent developments at X/Open concerning the UNIX API also bear watching.

11. SECURITY SERVICE STANDARDS[59]

This chapter summarizes the status of standards in security. Appendix F identifies organizations and standards bodies that have contributed to development of these standards.

11.1 Requirements for Security

Security services protect the components, mechanisms, and information of the AIS. Basic security features include authentication, access control, confidentiality, integrity, and non-repudiation.

Security features are required by both civil and military systems and are being addressed in some areas by standards bodies. Specific military requirements for security and the TSGCE recommendations for addressing these requirements are treated in Section 17.3.5.

11.2 Status of Standards for Security

11.2.1 Overview of Civil and Military Security Standards

Standards for security are being addressed in the following (details are provided in sections that follow):

- ISO 7498-2, *Security Architecture,* February 1989.
- ISO/IEC 10181, *Security Frameworks in Open Systems,* January 1992.
- *NATO OSI Security Architecture (NOSA),* March 1988, UNCLASSIFIED [Ref. NOSA 1988], defines the security services, based upon ISO 7498-2, required in the NATO OSI Reference Model; to be issued for ratification in revised form as STANAG 4250-2.
- *Security Architecture for NATO Information Systems Interconnection (SANISI),* Version 2.0, April 1989, NATO CONFIDENTIAL [Ref. SANISI 1989], which includes a description of the Trusted Communications Sublayer (TCS).
- Security annexes (Annex B) for NATO OSI STANAGs 4250-56 and 4261-66 and other STANAGs planned for Layers 6 and 7 (a draft Annex B has been prepared for STANAG 4253 and 4263).
- *Generic Upper Layer Security (GULS)* (DIS 11586) comprises security exchange service element and presentation [SC21 N 6992, SC21 N 6993, SC21 N 6994, and SC21 N 6995].
- ITU-TS X.800 *Security Architecture for Open Systems Interconnection for ITU-TS Applications* (a complete list of X.800-series standards is provided in Appendix E at the end of Section II).

59 An early (January 1994) draft of this chapter was informally reviewed by Mr. Hal Staton, National Security Agency, Chair of TSGCE SG9 Ad Hoc Working Group on Security.

- Lower layer security protocols, including the *Network Layer Security Protocol* (NLSP, ISO 11577, November 1993) and the *Transport Layer Security Protocol* (TLSP, ISO 10736, November 1993). [Ref. Curcio 1994] (There is a close correspondence of services between the NLSP and TCS [Ref. PC 1989]; future work in TSGCE SG9 on the TCS will be based on the NLSP [Ref. Staton 1994].)
- IEEE P1003.6 and JTC1 SC22 standards for POSIX security (see Section 10.2.1).
- ANSI X3.172A-199x, *Computer Security Glossary--Addendum to American National Standard Dictionary for Information Processing Systems,* is currently undergoing review
- MIL-STD-2045-18500, *Information Technology - Defense Standardized Profiles AMHxn(D) - Message Handling Systems - Message Security Protocol,* Draft, 1993 (defines a profile of standards to be used by defense message systems requiring a message security protocol) [Ref. Curcio 1994].

11.2.2 Security Standards Work in ISO[60]

SC21/WG1, SC21/WG3, and SC21/WG6 have begun a number of initiatives to address the models and standards frameworks required to progress OSI security standards. These include [SC21 N 8380 1993]:

- *OSI Security Architecture* (ISO 7498-2), February 1989—defines the general security-related architectural elements that can be applied appropriately in the circumstances for which protection of communications is required; provides a general description of security services and related mechanisms (e.g., authentication, access control, non-repudiation, integrity, confidentiality); and defines the positions within the OSI Reference Model where the services and mechanisms may be provided.
- *Guide to Open Systems Sec*urity, December 1993 [SC21 N 8380], a technical report developed to (1) define the scopes of the OSI security frameworks and upper and lower layer security models and (2) provide an overview of the security-related work within SC 21.
- *Security Frameworks in Open Systems* (ISO/IEC 10181, eight parts)—provides comprehensive and consistent descriptions of specific functional areas of security (e.g., authentication and access control), addressing all aspects of these areas in relation to how they may be applied in the context of a specific architecture (see Section 11.2.2.1).
- *Network Layer Security Protocol* (NLSP, ISO/IEC 11577, November 1994) and *Transport Layer Security Protocol (TLSP*, ISO/IEC 10736, November 1994)—define security protocols for Layers 3 and 4, respectively (see Section 11.2.2.2).
- *Upper Layer Security Model* (ISO/IEC 10745)—provides standards developers with the architectural model for development of application-independent services and protocols for security in the upper layers of OSI and the use of these services and protocols to fulfill the security requirements of a wide variety of applications, so that the need for application-specific A SEs to contain internal security services is minimized. The model addresses su| port, positioning, and relationship of security services and mechanisms; interactions among layers in providing and using security services, management of security; security policy; and security state. It includes handling of security transformation functions (e.g., encipherment) and security check-value functions from the Application and Presentation Layers. (See Section 11.2.2.1.)

60 Based on December 1993 edition of the *Guide to Open Systems Security* [SC21 N 8380].

- *Lower Layer Security Model* (SC21 N 7951)—intended to provide standards developers with the necessary basis for the development of security-related protocol and protocol elements appropriate to the lower layers of the OSI Reference Model. Development of this model has been deferred by SC6 (see Section 11.2.2.2).
- *Generic Upper Layer Security* (GULS, DIS 11586, six parts), which includes the Security Exchange Service Element (SESE)—defines a set of generic facilities to assist in the provision of security services in OSI applications. GULS includes a set of notational tools to support the specification of selective field protection requirements in abstract syntax specification and the specification of security exchanges and security transformations; service definition, protocol specification, and PICS proforma for SESE; and specification and PICS proforma for a security transfer syntax (see Section 11.2.2.4).
- Association Control Service Element (ACSE) authentication service (ISO 8649/AM 1) and protocol (ISO 8650/AM 1)—provides a field that can be used to carry arbitrary authentication information in a request and a confirmation.
- *Management Plan for OSI Security Activities* (SC21 SD-7, June 1990).

Other work is progressing in SC21 on security enhancements to presentation standards, to association control standards, and (as necessary) to other standards:

- Alignment of upper and lower layer security protocols (SC21 N 6996)
- ASN.1 encoding rules to provide upper layer security and compression (SC21 N 6130)
- Authentication and related security services for distributed applications (SC21 N 6099) (see Section 11.2.2.13)
- CMIS access control (ISO 9595/AM 4) and CMIP access control (planned amendment to ISO 9596-1; see Section 11.2.2.10)
- Directory access control (ISO 9594-1/AM 1, ISO 9594-2/AM 1, ISO 9594-3/AM 1, ISO 9594-4/AM 1, and ISO 9594-8/AM 1) and Directory authentication (ISO 9594-8) (see Section 11.2.2.8)
- FTAM security services (work suspended; see Section 11.2.2.5)
- *Generic Security ESO-OSI (External Security Object-Open Systems Interconnection) Abstract Interface Standard* (see Section 11.2.2.12)
- Objects and attributes for access control (ISO/IEC 10164-9; see Section 11.2.2.10)
- Open Distributed Processing (ODP) security (see Section 13.2)
- Positioning of encipherment and decipherment functions (Application Layer versus Presentation Layer) (SC21 N 5503)
- Presentation confidentiality and integrity (SC21 N 5059)—being progressed as amendments to ISO 8822 and ISO 8823
- *Reference Model of Data Management* (ISO 10032; see Section 11.2.2.9)
- *Remote Data Access* (ISO 9579; see Section 11.2.2.9)
- *Security Alarm Reporting Function* (ISO/IEC 10164-7; see Section 11.2.2.10)
- *Systems Management Overview* (ISO/IEC 10040; see Section 11.2.2.10)
- TP security (work suspended; see Section 11.2.2.6).

SC17/WG4 is developing security services for integrated circuit (identification) cards (ISO 7816). SC18 is developing security features for Message Oriented Text Interchange (MOTIS, ISO/IEC 10021); Distributed Office Applications and Management (DOAM, ISO/IEC 10031); Document Filing and Retrieval (DFR, ISO/IEC 10166); and Document Printing

Application (DPA, DIS 10175). SC22/WG15 is developing a security interface for POSIX (SC22/WG15 N 46R1)

SC27, Security Techniques is also working with SC21 on several projects [Ref. SC21 N 6066 1991]:

- *Data Encipherment - Physical Layer Interoperability Requirements*, February 1988 (ISO 9160)
- *Data Integrity Mechanisms Using a Cryptographic Check Function Employing a Block Cypher Algorithm* (ISO/IEC 9797)
- *Digital Signature Scheme Giving Message Recovery*, 1991 (ISO 9796)
- *Entity Authentication Mechanisms* (ISO/IEC 9798)
  - ISO/IEC 9798-1 (Part 1): *General Model*
  - DIS 9798-2 (Part 2): *Entity Authentication Mechanisms Using Symmetric Algorithms* (draft proposed standard)
  - DIS 9798-3 (Part 3): *Entity Authentication Using a Public Key Algorithm*
  - WD 9798-4 (Part 4): *Entity Authentication Using Non-Reversible Functions*
  - WD 9798-x (Part x): *Entity Authentication Using Zero-Knowledge Techniques*
- *Guidelines for Management of IT Security* (PDTR 13335)
- *Hash Functions*, 1993 (DIS 10118):
  - DIS 10118-1 (Part 1): *General Model*
  - DIS 10118-2 (Part 2): *Hashing Operation Using Symmetric Block-Cipher Algorithm*
  - WD 10118-3 (Part 3): *Dedicated Hash Functions*
  - WD 10118-4 (Part 4): *Hash Functions Using Modular Arithmetic*
- *Key Management* (CD 11770 and WD 10181-8); the parts of CD 11770 are:
  - WD 11770-1 (Part 1): *Framework*, 1993 [SC27 N 685]
  - CD 11770-2 (Part 2): *Key Management Mechanisms Using Symmetric Techniques*, November 1992 [SC27 N 626]
  - CD 11770-3 (Part 3): *Key Management Mechanisms Using Asymmetric Techniques*, 1993
- *Modes of Operation for 64-bit and n-bit Cipher Algorithms* (ISO 8372 and ISO/IEC 10116)
- Non-repudiation mechanisms (SC27 N 209)
- *Procedures for the Registration of Cryptographic Algorithms*, 1991 (ISO 9979)
- *Security Information Objects (SIO)* [SC21 N 686]
  - Part 1: *Method and Guidelines for the Definition and Registration of Security Information Objects*
  - Part 2: *Elements and Generic Security Information Object Class Specifications*
- *Specific SIO Class Definitions* [SC27 N 429, April 1992], working draft.
- *Zero Knowledge Techniques* [SC27 N 345, November 1991]—the means by which possession of information can be verified without any part of that information being revealed, whether to the verifier or to any third party. (These techniques are applicable to entity authentication, data authentication, and digital signature.)

TC68, Banking and Related Financial Services, has two subcommittees working on security standards. TC68/SC2, Operations and Procedures, is developing standards for message authentication (ISO 8730 and 8731), key management (ISO 88732), message encipherment (ISO/IEC 10126), sign-on authentication (ISO/IEC 11131), and data security framework (ISO 11166). TC68/SC6, Financial Transaction Cards, Related Media, and Operations, is

developing standards for message authentication (ISO 9807), pin management (ISO 9564), key management (ISO/IEC 11568), and cryptographic devices (ISO/IEC 13492), and integrated circuit cards (ISO/IEC 10202 and WD 13182). Listings of the parts and titles of these standards are provided in Appendix D (Section I.D) and Appendix E.

11.2.2.1 Security Frameworks

ISO/IEC 10181, *Security Frameworks in Open Systems*, defines the framework within which security services for open systems are specified. These open systems include database, distributed applications, ODP, and OSI. The framework addresses data elements and sequences of operations (but not protocol elements) that are used to obtain security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems and to data managed by systems. The security frameworks are intended to provide guidance to standards developers and are not implementable standards against which conformance can be claimed [SC21 N 7089]. Note that the security framework is being developed by SC21/WG1, with SC27 developing Part 8, *Key Management*. Table 34 identifies the scope of individual parts of the framework. Initiation of ITU-TS approval for these parts is expected in November 1994.

In a 1992 statement on scope and usability of the *Security Frameworks for Open Systems*, SC21/WG1 agreed on the following points as a basis for expediting the frameworks and improving their usefulness [Ref. SC21 N 7089 1992]:

- The concept of including some "compliance" wording with each framework was generally (though not unanimously) agreed to be a useful step in making known the objectives of the standard.
- Reference to specific styles of implementation should be non-normative, illustrative, not definitive, and should be confined to examples only. No attempt should be made to provide complete sets of possible implementations.

The United Kingdom feels strongly that if the security framework is to be used by OSI, ODP, or database applications, some element of standardization is necessary to determine the way in which each part of the security framework is to be applied, using the concepts and terminology of the relevant area. It sees the application of the authentication, access control, and audit frameworks to OSI as the most urgent requirements. [Ref. BSI 1991]

11.2.2.2 Security Models and Protocols[61]

The purpose of the security models is to apply the security concepts detailed in the Security Frameworks to specific areas of open systems architectures.

Lower Layers Security Model. While an OSI Lower Layer Security Model [SC6 N 5333] was begun, it was decided at a joint meeting of SC6/WG2 and SC6/WG4 in October 1990 not to progress it. The purpose of the model was to provide standards developers with the necessary basis for the development of security-related protocol and security-related protocol elements appropriate to the lower layers of the *OSI Basic Reference Model*. The model would address concepts, guidelines, interactions, and management requirements. *Security in Lower Layer Protocols and Guidelines* [SC6 N 6957] may form the basis of a future standard. A number

[61] Discussion for this section was taken from the January 1991 *Guide to Open Systems Security* [SC21 N 5533] and updated based on the December 1993 edition of this document [SC21 N 8380].

of security issues need to be resolved before this would be likely. [Ref. SC6 N 6219 1990; Walters 1991]

Table 34. OSI Security Frameworks—ISO/IEC 10181

- Part 1 (CD 10181-1.2), *Overview*, June 1993 [SC21 N 7083]—Describes the organization of the security framework, defines security concepts (e.g., domains, authorities, policies) that are required in more than one part of the security framework, and describes the interrelationship of the services and mechanisms identified in other parts of the framework. Initiation of ITU-TS approval expected November 1994.
- Part 2 (ISO/IEC 10181-2), *Authentication Framework*, June 1993 [SC21 N 7853]—Authentication is the process of corroborating an identity. The standard defines basic concepts, identifies possible classes of mechanisms, defines services, identifies functional requirements for protocols, identifies management requirements, and aligns terminology and concepts with ISO/IEC 9798, *Entity Authentication Mechanisms*. Two amendments are in WD status: *Refinement of Subcomponents of Claimant and Verifier* and *Classification for a New Class of Mechanisms to Defeat Opportunistic Attacks*. A new work item on *Authentication Elements*, which would be an amendment, has been proposed.
- Part 3 (DIS 10181-3), *Access Control Framework*, September 1993 [SC21 N 8224]—Access control is the process of determining that uses of resources within an open system environment are permitted and, where appropriate, preventing unauthorized access. Accesses may be to a system or within a system.
- Part 4 (DIS 10181-4), *Non-Repudiation Framework*, December 1993 [SC21 N 8378]—Non-repudiation is a security service that provides proof of origin or delivery of data in order to protect the sender against the false denial by the recipient, that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent. The use of appropriate mechanisms is coupled with the necessary assurance mechanisms providing proof about certain properties of the communications between the entities involved, such as its integrity, origin, time, and destination. Non-repudiation implies the existence of an agreed third party whose primary role is to arbitrate disputes resulting from non-repudiation.
- Part 5 (DIS 10181-5), *Confidentiality Framework*, February 1993 [SC21 N 7602]—The maintenance of the secrecy of data is called confidentiality.
- Part 6 (DIS 10181-6), *Integrity Framework*, February 1993 [SC21 N 7603]—The integrity framework addresses the constancy of a data value and not any other form of invariant that such a value may possess. In particular, it does not address the constancy of any information that the data is deemed to represent. There are two types of integrity mechanisms needed for two types of constancy. The first is the constancy of the value of data in an environment in which a *random* modification to integral data may be made. The second is the constancy of the value of data in an environment in which a modification to integral data may *deliberately* be made to defeat the integrity mechanism.
- Part 7 (CD 10181-7.2), *Security Audit Framework*, March 1993 [SC21 N 7685]—This second CD describes a model of a system's audit trail, a description of audit events and the different types of information involved, and its relationship to management activities.
- Part 8 (WD 10181-8), *Key Management*, November 1991 [SC21 N 6066—Work on this part is being carried out in SC27. The purpose of key management is to provide procedures for handling cryptographic keying material to be used in symmetric or asymmetric cryptographic mechanisms. Key management includes: key generation, key distribution, key installation, key storage, key archiving, and key deletion. A fundamental problem is to establish keying material whose origin, integrity, and, in the case of secret keys, confidentiality can be guaranteed. The work addresses, in part, the concern about proliferation of protocol-specific key management mechanisms.

Sources: ISO/IEC 10181 and *Guide to Open System Security* [SC21 N 8380].

The issue of adding security services to Layer 2 in ISO 7498-2 was raised by SC21/WG1 in May 1991. The IEEE standard for Interoperable LAN Security (802.10 Part B) provides data confidentiality, connectionless integrity, data login authentication, and access control security services at OSI Layer 2, while ISO 7498-2 provides only data confidentiality. The relevant document is, *Data Link Layer Security* [SC6 N 6927; SC21 N 6346]

Network Layer Security Protocol (ISO 11577). The NLSP is based on three standards efforts. One part of the US Secure Data Network System[62] (SDNS) is a connectionless

62 One of the objectives of SDNS is to emphasize commercial participation in developing security products.

Layer 3 security protocol (SP3) equivalent to the end-to-end encryption portion of the TCS identified in draft STANAG 4250-2 and described in SANISI. Northern Telecom's SPX security protocol adds connection-oriented service to SP3. The United Kingdom's End-to-End Security Protocol (EESP) adds connection-oriented services to SP3 and includes integrity and traffic padding.

NLSP can operate both in the CO and CL modes and can be implemented in both end systems and intermediate systems. Both modes support address (source/destination) confidentiality. The NLSP protocols makes use of the concept of a security association (for cryptographic keys and associated parameters) and provides security on the basis of the quality of service the Transport Layer demands and the quality of service the domain administration proposes. In October 1993, the SC6 plenary agreed to approve the NLSP for IS status [Ref. Curcio 1994].

Transport Layer Security Protocol (ISO 10736). TLSP is based on the SDNS Layer 4 security protocol (SP4) and specifies optional extensions to both the connection-oriented transport protocol (ISO 8073) and connectionless-mode transport protocol data unit (TPDU) transmission (ISO 8602) standards to permit use of cryptographic techniques. Since the protocol operates as an extension only, it does not preclude unprotected communication between transport entities implementing ISO 8073 or ISO 8062. In October 1993, the SC6 plenary agreed to approve the TLSP, together with Amendment 1, *Exchange of Security Attributes*, for IS status [Ref. Curcio 1994].

Upper Layers Security Model (ISO 10745). The *Upper Layer Security Model* provides the necessary basis for the development of security-related protocol elements for the secure exchange of information between open systems, with the interchange of information related to security policy control and management, and with services and mechanisms for controlling access to resources accessible via OSI. It addresses the following:

- Security aspects of communication in the upper layers of OSI
- Relationships between security services and mechanisms in the upper layers, to be considered in greater detail than is provided in ISO 7498-2
- Properties of the possible combinations of security services and mechanisms in the upper layers
- Interactions among Application, Presentation, and Session Layers in providing security services
- Invocation of lower layer security services
- Requirements for security management in the upper layers.

The *Upper Layer Security Model* (ISO 10745) recently progressed to ISO status. It addresses primarily FTAM security requirements, not those of distributed applications such as Directory, TP, and X.400. [Ref. X3 1991o]

11.2.2.3 Requirements and Approaches for Security

In March 1990 at the Workshop on Distributed Applications in Phoenix, the following observations on security were made [Ref. SC21 N 4526 1990]:

- It is highly desirable to standardize a general approach to providing security in the Application Layer. This can be accomplished by supporting a variety of security methods that involve communication of security information, such as two-way or

three-way authentication exchange, privilege attribute certificate transfer, and key negotiation sequence.

- A security method would consist of semantics, syntax, and procedural rules relating to the communications aspects of the method.
- There appear to be three possible OSI architectural approaches to supporting security methods:
  - No generic security ASE(s), in which the syntax and procedural rules for any security method are imported into the specification of an application-specific ASE.
  - One generic ASE, in which one ASE is provided that can import into its abstract syntax the syntax of any security method.
  - Multiple purpose-specific security ASEs, in which each ASE incorporates the procedural rules and syntax for a particular security method or group of closely related methods (e.g., an ASE to support two-way authentication exchanges).
- Satisfaction of security requirements of TP, Directory, and OSI Management will depend on addressing security modelling issues related to distributed applications.
- Access control to data resources must address the data model being used by individual applications such as DFR, DTAM, FTAM, IRDS, RDA, SQL, etc. Use of a common data modelling approach provides the potential for use of common access control facilities to such data resources and consequently increases the attractiveness of the common data model approach in order to prevent the need for re-specification of access control facilities for data management applications.

11.2.2.4 Security Exchange and Generic Upper Layer Security

SESE. A security exchange is the transfer of protocol-control-information, called security exchange information, between open systems as part of the operation of a security mechanism. An ASE that supports the communication of security exchange information is designated a Security Exchange Service Element (SESE). SESE will provide for the transfer of information between a pair of application-entity invocations in support of security services such as authentication, access control, confidentiality, and integrity. The security exchange would be allowed to occur either in conjunction with association establishment or at any time on an established association. Encryption/signature functions could be located in either the Application Layer or the Presentation Layer. SESE includes a standard method for defining security exchange information using ASN.1[Ref. SC21 N 5002 1990]

GULS. ITU-TS Q19/7 and WG6 have decided to progress the SESE and Presentation Layer security documents together as a multi-part standard on Generic Upper Layers Security (GULS). GULS will comprise six parts:

- DIS 11586-1 (Part 1): *Security Exchange Overview and Specification Framework*, August 1993 [SC21 N 8182]
- DIS 11586-2 (Part 2): *Security Exchange Service Element (SESE) Service Definition*, August 1993 [SC21 N 8183]
- DIS 11586-3 (Part 3): *Security Exchange Service Element (SESE) Protocol Specification*, August 1993 [SC21 N 8184]
- DIS 11586-4 (Part 4): *Protecting Transfer Syntax Specification*, August 1993 [SC21 N 8185]
- WD 11586-5 (Part 5): *Security Exchange Service Element (SESE) PICS Proforma*, June 1993 [SC21 N 7912]
- WD 11586-1 (Part 6): *Protecting Transfer Syntax PICS Proforma*, June 1993 [SC21 N 7913].

11.2.2.5 FTAM Security

FTAM security services were the subject of standardization work in SC21 during 1990 to 1992, but this work was suspended in June 1993. *Enhancements to FTAM Security Services* [JTC1 N 955] (the new work item proposal), *Security Aspects of FTAM* [SC21 N 6811, March 1992], and ISO 8571-1/WDAM 5, *Enhanced Security for FTAM* [SC21 N 7927, May 1993] were examples of the work completed, generally based on use of passwords and access control lists. Suspension was due to lack of resources and the emerging GULS standard.

FTAM-specific requirements include the need for an overall security policy in FTAM so that any changes become part of a coherent whole. Possible extensions that could be made to the existing FTAM protocol and service include authentication, access control list, mandatory or label based access control, change attribute, and filestore management.

11.2.2.6 TP Security

Transaction Processing Security—a new work item that was suspended in June 1993—addressed the formulation and provision of mechanisms to meet a number of security services, including authentication, access control, confidentiality, integrity, non-repudiation, auditing, "management," access right revocation, replay protection, prevention of the denial of service, reliability, and traffic flow confidentiality. Suspension was due, in part, to concerns about alignment of early work with ISO 7498-2 and the emerging SESE in GULS (DIS 11586).

11.2.2.7 ODA Security

Changes are being made to ODA, ISO 8613, to improve the security aspects. ODA provides protection for documents as a whole or for parts of a document. Confidentiality, integrity, authentication, and non-repudiation of origin are all supported using encipherment, fingerprints, and seals. [Ref. SC21 N 4472 1990]

11.2.2.8 Directory Security

ISO 9594-1/AM 1, ISO 9594-2/AM 1, ISO 9594-3/AM 1, and ISO 9594-4/AM 1 develop a model for access control and an access control scheme for general use (in Part 2) and (in Parts 3 and 4) provides "hooks" whereby the access to directory information can be controlled. Hooks inserted by the amendments to Parts 3 and 4 allow a variety of external access control schemes to be used, in addition to the basic access control scheme of Part 2. The *Directory Authentication Framework* (ISO 9594-8) describes a security token protected by integrity and data origin authentication security services called a certificate. The mechanism used to provide this protection involves the use of public key cryptosystems. Three authentication exchange mechanisms are defined to provide unilateral or mutual authentication.

A new work item, *Security Enhancement to Directory* failed to qualify for acceptance to the JTC1 work program, but has been incorporated into another NWI, *Authentication and Related Security Services for Distributed Applications* (see Section 11.2.2.13). However, a new work item proposal, *Enhancement of Directory Operational Security*, has met the criteria for acceptance into the JTC1 program of work, and SC21 has been requested to respond to the comments received. The June 1993 draft is SC21 N 7932. It would result in addenda to ISO 9594-1 through ISO 9594-9 and possibly one new part. Target dates are as follows: WDAM in November 1994, PDAM in October 1995, DAM in October 1996, and AM in October 1997. Section 9.11.7.3 describes a related new work item proposal for Certificate Definitions [SC21 N 7102].

11.2.2.9 Database and Data Management Security

SQL. SQL2 specifies some security functionality, but the standard (ISO 9075) does not address how a secure database should be built. ISO 9075 does provide user authorization parameters for users of SQL data and services.

Remote Data Access (RDA). RDA (ISO 9579-1) allows interactive access to a remote database from a terminal and carries the user identity and authorization identity in the request/indication service primitives when an RDA dialogue is being set up with a remote node—the dialogue is rejected if either the user or authorization identities are found to be invalid. RDA does not dictate the format or meaning of this security-related information.

POSIX. Since the security of the operating system needs to be considered in building a (secure) database, POSIX standards are also relevant to the security of databases.

Reference Model of Data Management (RMDM). ISO/IEC 10032 (RMDM) describes access control in terms of privileges, provides an architectural model in which access control data are considered similar to database data, and lists a standardized approach to access control as a technical objective associated with data management standardization. Access control is the only security service supported within the scope of data management, although requirements for other security services are identified in ISO/IEC 10032.

Information Resource Dictionary System (IRDS). An IRDS documents and controls an enterprise's information resources. Access to an information resource dictionary is required to be limited, and the ISO/IEC 10027 (*IRDS Framework*) characterizes the criteria that might be used to decide access. ISO/IEC 10728 (*IRDS Services Interface*) specifies mechanisms for interfaces to IRDS services.

11.2.2.10 Management Security

A brief amendment (AM 4) on access control has been added to ISO 9595, *Common Management Information Service (CMIS) Definition.* It specifies the presence and purpose of access control parameters, but it does not define the nature or format of the parameters. ISO/IEC 10040 (Systems Management Overview) identifies security management functions and relates them to the OSI Reference Model and the framework for audit. Three parts to ISO/IEC 10164 (*Systems Management*) specify security services for OSI management: *Security Alarm Reporting Function* (Part 7), which can be used by applications using CMIS to raise security alarm events based on the *Alarm Reporting Function* (Part 4); *Security Audit Trail Function* (Part 8), in which event reports are sent to an audit trail log; and *Objects and Attributes for Access Control* (Part 9), which models the provision of access control to management objects at a target end system.

11.2.2.11 International Standardized Profile (ISP) Security

It has been suggested that the scope of TR 10000 be extended to address the security features in ISPs. An ISP may contain security features if one (or more) of the base standards to which it refers contain security features. In general, the specification of an ISP having security features has two distinct parts, one concerned with security-related functions and one concerned with other functions. This specification is referred to as a security sub-profile. An ISP may contain one (or more) security sub-profiles. The security sub-profile comprises [Ref. Humphreys 1991]:

- A description of the target system environment in which the sub-profile is intended to be used
- An identification of the range of (security) threats that the sub-profile is intended to counter in the target system environment
- A specification of how security functions in base standards should be used to counter the assumed threats
- A specification of the security mechanisms that should be used to provide the necessary security functions (where the base standards provide some freedom of choice)
- A specification of the range of the realizable quality attainable through the use of this sub-profile.

11.2.2.12 Generic Security ESO-OSI (External Security Object-Open Systems Interconnection) Abstract Interface Standard

The UK originally proposed this standard in a work plan for the security of distributed applications. The strawman document [SC21/WG6 N 1158] defines an abstract interface between two types of specifications for ISO application security: (1) an OSI application protocol specification including enhancements for security and (2) a specification for a security support function based on a specific set of mechanisms (i.e., ESO in terms of the Upper Layers Security Model). It is based on a Generic Security Service API proposed to the Internet Common Authentication Technology WG, although this document does not define itself as a concrete API. [Ref. SC21 WG6 N 1158 1992]

11.2.2.13 Additional Security Standards Work in ISO

Conformance Testing. The UK contributed a discussion paper on Conformance Testing for OSI Security to the SC21/WG1 meeting in Ottawa in May 1992. The paper supports the establishment of a new question on Conformance in OSI Security to define the scope of work to be done on this topic in SC21 and to get this agreed with SC27, to ensure proper coordination of the SC21 activity with related SC27 work. [Ref. SC21 WG1 N 1140 1992] A majority of national bodies voting on Q1/69,[63] Conformance Assessment for OSI Security, support work on this proposed new question. [Ref. SC21 N 7473 1992]

Authentication and Related Security Services for Distributed Applications. In June 1991, a new project was proposed to define an authentication service for distributed applications in an open systems environment [SC21 N 6099]. However, the NP ballot failed to receive the required level of commitment by National Bodies for work to proceed. For the same reason, a related project, *Security Enhancements to the Directory Authentication Framework* [SC21 N 6172] also failed. The United States therefore suggested merging the two efforts and an NP to that effect (*NWI on Authentication and Related Security Services for Distributed Applications*) has met the criteria for acceptance into the JTC1 Program of Work and has been assigned to SC21/WG8 for development. [Ref. SC21 N 7580 1993]. An early draft is SC21 N 7914, *Working Document on Authentication and Related Security Services*, August 1993. This standard will define services for distributed applications in an Open Systems Environment to support authentication, access control, and key management. A five-part international standard is being contemplated with target dates as follows: CD expected

---

63 Questions are used to direct new work; a list of questions for SC21 is provided in Section 2 of Appendix G.

December 1994, DIS December 1995, and IS December 1996. The parts are *Model, Generic Abstract Service, Security Application Service Definitions, Protocols,* and *PICS Proforma.*

The scope of the standard for authentication and related security services will include a key distribution protocol (KDP). The NIST will support the development of a working draft document based on the IEEE 802.10 Key Management Group [Ref. Curcio 1994]

Generic Abstract Services for Security (GASS). While the primary basis of work on authentication will be ISO 9594-8, it is anticipated that ECMA-138 (see Section 11.2.4.3) will also provide a useful basis for these services. The strawman document for Part 2 of the standard, *Generic Abstract Services for Security (GASS)* is SC21/WG8 N 173, November 1993. ECMA/TC36-TC9 has contributed an early draft of a three-part standard on *Authentication and Privilege Attribute Security Application with Related Key Distribution Functions,* November 1993. The three parts are *Overview and Functional Model* [SC21 N 8325], *Security Information Objects* [SC21 N 8326], and *Service Definitions* [SC21 N 8327].

Authentication for Lower Layers. SC21/WG8 has noted that the authentication is aimed primarily for upper layer security protocols, it is also expected to support the lower layer security protocols. The concept of a security association will be a central concept, defined as a relationship between two or more entities for which there exist attributes (static and dynamic information and rules) to govern the provision of security services involving those entities. [Ref. SC21 N 7915 1993]

11.2.3 Security Standards Work in NATO

11.2.3.1 TSGCE SG9 AHWG on Security

The TSGCE SG9 Ad Hoc Working Group (AHWG) on Security developed the NOSA and SANISI documents (identified in Section 11.2.1 above), whereas the security annexes for the layer STANAGs are the responsibility of TSGCE SG9/WG5 and SG9/WG6. NOSA was developed to give guidance to contractors and procurement managers on the preferred placement of security services within OSI-conformant systems. SANISI provides more detailed rationale on the placement of security services and mechanisms within the NATO OSI Reference Model. Section 17.3.5.1 provides a description of the current work of the AHWG on Security.

11.2.3.2 NATO OSI Security Architecture (NOSA)

NOSA identifies OSI security services for the Physical, Network, and Presentation/Application Layers. These are [Ref. NOSA 1988]:

- Physical Layer will provide two services by transparent means without requiring modifications to the Physical Layer protocols:
  - Connection confidentiality, which is capable of dealing with circumstances where the physical communication is intermittent or asymmetric.
  - Traffic flow confidentiality.
- Network Layer security services are provided within subnetwork-dependent roles and within a TCS:
  - Subnetwork-dependent services are peer entity authentication, data origin authentication, access control, connection confidentiality, connectionless confidentiality, traffic flow confidentiality, connection integrity without recovery, and connectionless integrity.
  - Security services that can be provided by the NATO TCS are identical to the eight identified above for subnetwork-dependent roles.

- Presentation/Application Layers could provide as many as 14 security services:
  - The eight services identified above for the Network Layer.
  - The following additional six services: selective field confidentiality, connection integrity with recovery, selective field connection integrity, selective field connectionless integrity, non-repudiation with proof of origin, and non-repudiation with proof of delivery.

NOSA is the basis for Part 2 of the NATO OSI Reference Model (STANAG 4250-2): *Security*, Version 4.0, 9 December 1993. Draft STANAG 4250-2 supersedes NOSA. Documentation of the NATO security architecture for voice and video communications (e.g., ISDN) is being developed separately and may become a supplement to STANAG 4250-2.

11.2.4 Other Security Standards Work

11.2.4.1 Secure Data Network System (SDNS)

The Secure Data Network System (SDNS) was established in 1986 as a partnership between NSA and 10 major computer and telecommunications companies, including AT&T, Digital Equipment Corporation, and IBM, with the goal of developing a security architecture based on the OSI model and using a distributed key generation system in which computers are able to establish cryptographic keys as needed to communicate with other computers. [Ref. RNLA 1994, p. 126] The goals of SDNS were to create specifications for end-to-end security; to use the OSI Reference Model; to design an architecture to include electronic mail and end-to-end encryption; to provide transparent key management; and to demonstrate feasibility of techniques. The US National Security Agency (NSA) supported the SDNS project, which has released to the public domain several standards for security protocols [Ref. NSA 1989 and 1989 a-j]. (SDNS is no longer being actively supported by NSA—all work related to SDNS has now been referenced to NLSP, TLSP, and the Message Security Protocol (MSP).

SP3 and SP4 have been introduced into the ISO voluntary standard process by ANSI. SP3 has evolved into ISO 11577, Network Layer Security Protocol (NLSP) and SP4 has evolved into ISO 10736, Transport Layer Security Protocol (TLSP). Even though the protocols have retained the same functionality as their SDNS counterparts, changes introduced during the standards process have made NLSP non-interoperable with SP3 and TLSP non-interoperable with SP4. The SDNS standards for SP3, SP4, MSP, and others is provided in Table 35.

Some of the differences between the international standard protocols (NLSP and TLSP) and the SDNS protocols are as follows [Ref. Walters 1993]:

- NLSP and TLSP use variable-length fields to carry Type, Length, and Value data in each Protocol Data Unit (PDU) while SP3 and SP4 use fixed-length, fixed-position fields. This gives NLSP and TLSP greater flexibility (and higher overhead) since field lengths can be changed and field order varied by making a parameter change rather than redefining the protocol.
- SP3 supports DoD IP using the SP3-D variant in addition to the ISO Connectionless Network Protocol (CLNP) (ISO 8473). NLSP only supports CLNP. SP3 support for DoD IP is critical to the US Government's installed base of end systems that implement DoD IP. However, as new procurements filed US GOSIP-compliant end systems, the proportion of DoD IP end systems is expected to shrink relative to ISO CLNP end systems.
- NLSP can support Connection Oriented Network Service (CONS) whereas SP3 cannot.

- NLSP and TLSP support Security Association (SA) - Protocol (SA-P) as an option that allows NLSP and TLSP peer entities to exchange information needed for SA establishment and rekeying during the lifetime of an SA and an SA release.
- TLSP uses double encapsulation, which increases overhead.
- SP4 has an optional Final Sequence Number (FSN) field in the protected header. SP4 validates the FSN to ensure complete shut down of a session. TLSP does not support FSN, leaving this function to the session layer protocol. This raises prospects of allowing successful attacks if the session layer does not ensure that the last packet of a connection has been properly received and acknowledged. However, specifying a properly implemented session layer protocol above TLSP will provide the same service as FSN.
- TLSP can support protected header field sizes up to 65,535 octets, while SP4 can only support sizes up to 254 octets. However, the SP4 protected header field is followed by an encapsulated Transport PDU of unlimited length. This larger protected content field size supported by SP4 provides a more efficient data transfer method than TLSP since more data can be carried in each SP4 Secure Data Unit."

Table 35. Security Protocols Developed in SDNS

- Security Protocol 3 (SP3). Provides various security services in the Network Layer through the use of cryptographic mechanisms; SP3 is a subnetwork independent convergence protocol (SNICP, ISO 8648) that extends the CLNS (ISO 8348/AD1) with confidentiality (protection against passive monitoring), integrity (protection against modification, replay, addition, or deletion), or both. SP3 is designed to be used at the top of Layer 3 [Ref. NSA 1989].
- Security Protocol 4 (SP4). Specifies optional extensions of the COTS (ISO 8072) and connectionless transport service (ISO 8072/AD1) for the Transport Layer. The extensions permit the use of cryptographic techniques to provide data protection for transport connections for connectionless-mode Transport Protocol Data Unit (TPDU) transmission. SP4 can be used with the CONS or the CLNS. SP4 is designed to be used at the bottom of Layer 4 [Ref. NSA 1989a].
- Message Security Protocol (MSP). Defines additions to the ITU-TS X.400 (either 1984 or 1988) that permit any type of message (including interpersonal messages) to be sent and received securely. When used with the conventions defined by ANSI for the X.400 Message Transfer System, MSP can be used to exchange EDI messages securely. The MSP provides writer-to-reader confidentiality, access control for message transfer, and request for a signed receipt of the received message. SDN 701 [Ref. NSA 1989c] specifies the MSP, and SDN 702 [Ref. NSA 1989d] defines new attribute types and object classes for inclusion in the X.500 Directory in support of key management functions used by MSP.
- Key Management Protocol. Key management provides for the generation, distribution, and updating of traffic encryption keys (TEKs). The abstract model for a Key Management Application Process (KMAP) consists of two parts: the information processing part that is supported by Management Information Bases (MIBs) for keys and for TEKs, and the communication part, called the Key Management Application Entity (KMAE). The KMAE consists of the Layer 7 ACSE (ISO 8649) and a Key Management Application Service Element (KMASE). The Key Management Protocol provides Layer 7 peer-level services between the KMASEs of two KMAPs. The Key Management Protocol assumes the use of the connection-oriented presentation services (ISO 8822) [Ref. NSA 1989b; NSA 1989h; NSA 1989i; NSA 1989j].
- Access Control. Access control is the prevention of the unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner (ISO 7498-2). SDN 801, SDN 802, and SDN 802/1 [Ref. NSA 1989e; NSA 1989f; NSA 1989g] specify an access control framework based on a four-tiered model and an Access Control Information System (ACIS) that provides a uniform method for encoding access control information that is independent of any particular security policy. The ACIS also provides a standard algorithm for interpreting and comparing access control attributes. The access control framework provides for authentication data and access control checks that will allow communication between different SDNS users/systems when their respective security policies allow it. The framework provides two processes: a Peer Access Approval process for interpreting the data of the four-tiered mode, and the Peer Access Enforcement Process for enforcing access control on a Protocol Data Unit (PDU) basis [Ref. NSA 1989e; NSA 1989f; NSA 1989g].

11.2.4.2 NIST Recommendations

The NIST approach to OSI security standards includes the following features [Ref. DCA 1989a]:

- Security encapsulation standard to provide cryptographic protection of integrity and confidentiality. A common format and processing standard is needed that is independent of the algorithm to be used.
- Mail handling security system for MHS, to be used between the User Agent and the Transfer Agent to encapsulate the entire message contents; this requires posted keys and certificates. (One candidate is from X.411; another is the MSP from SDNS.)
- Cryptographic key management, a service to be provided at the Application Layer to support real-time (SP3 and SP4) as well as posted (MHS) requirements. FIPS 171, *Key Management Using ANSI X9.17*, was approved in April 1992.
- Security labels and labelling. These are planned to be strongly coupled with data.
- Authorization and access control. These features would permit policies to be specified within security domains and would support multiple policies and models (candidates are from ECMA and SDNS).

The NIST data encryption FIPS are as follows:

- FIPS 46-1, *Data Encryption Standard (DES)*, January 1988 (reaffirmed until 1992). This standard specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of computer data. The algorithm uniquely defines the mathematical steps required to transform computer data into a cryptographic cipher and the steps required to transform the cipher back to its original form. This standard has been adopted as a voluntary industry standard, ANSI X3.92-1981.[64] DES guidelines are provided by FIPS 74.
- FIPS 81, *DES Modes of Operation*, December 1980. This standard defines four modes of operation for the DES that may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). This standard has been adopted as a voluntary industry standard, ANSI X3.106-1983.
- FIPS 113, *Computer Data Authentication*, May 1985. This standard specifies a Data Authentication Algorithm (DAA) that, when applied to computer data, automatically and accurately detects unauthorized modifications, both intentional and accidental. Based on FIPS 46, this standard is compatible with requirements adopted by the Department of Treasury and the banking community to protect electronic fund transfer transactions.
- FIPS 139, *Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications*, August 1983. This standard facilitates the interoperation of government data communication facilities, systems, and data that require cryptographic protection using the DES algorithm. The standard specifies interoperability and security related requirements using encryption at the physical layer of the OSI Reference Model in the telecommunication systems conveying Automatic Data Processing and/or narrative text information. It is the same as US Federal Standard 1026 and ANSI X3.105-1983.
- FIPS 140-1, *Security Requirements for Cryptographic Modules, Equipment*, Draft May 1993. This standard prescribes security requirements for specifying cryptographic-based security systems used to provide protection for sensitive or valuable data. Protection of cryptographic modules within a security system is

[64] A list of ANSI standards is given in Section IV.C of Appendix H.

necessary to maintain the confidentiality and integrity of the information protected by the module. The standard specifies the security requirements that are to be satisfied by a cryptographic module..

- FIPS 141, *Interoperability and Security Requirements for Use of the Data Encryption Standard with ITU-TS Group 3 Facsimile Equipment,* April 1985. This standard specifies interoperability and security-related requirements for use of encryption with the ITU-TS Group 3-type facsimile equipment conveying Automatic Data Processing (ADP) and/or narrative text information. It is the same as US Federal Standard 1028.
- Digital Signature Standard (DSS). This standard satisfies the US Government's needs for cryptographic message authentication to protect its unclassified and unclassified but sensitive information processing infrastructure. DSS provides required authentication and non-repudiation services without unnecessarily putting trust in processing components.
- Common IP Security Option (CIPSO) Labeling Standard. The CIPSO allows the attachment of specific security attributes associated with the data in an IP datagram. These data are used to perform decisions at the IP layer. This document defines the basic format and processing procedures for the CIPSO. In addition, it defines the specific attribute formats and procedures to support the standard DoD Mandatory Access Control Security Policy. A FIPS based on this DoD standard is in preparation.

Finally, NIST is developing techniques outside the OSI model for personal identification and authentication. Approaches include knowledge, token, or physical means. Technologies being considered include a smart card and use of passwords. A NIST workshop in September 1990 addressed integrity guidelines.

The current concentration of NIST is on beginning the development of a new set of Information Security Product Evaluation Criteria, better known as the Federal Criteria. The first public draft of Federal Criteria (FC) for Information Technology (IT) Security was distributed in January 1993 for review and comment. The FC is the result of an ongoing joint effort between NIST and NSA. The FC is expected to evolve into a new FIPS and once approved will replace DoD 5200.28-STD *Trusted Computing Systems Evaluation Criteria (TCSEC)* or the Orange Book. The FC is published in two volumes. Volume I discusses *Protection Profile Development* and Volume II describes the *Registry of Protection Profiles.* Protection Profiles specify baseline requirements that meet generally accepted security enforcing functions with broad applicability and effectiveness. [Ref. CFS 1993]

The FC for IT Security provides a conceptual framework for defining requirements for trusted product development and evaluation. The framework is based on the definition of generic requirements for security functionality and security assurance expressed as primitive components or building blocks. The components can be combined into composite groups of requirements, or packages, and used to create unique sets of IT product security criteria called protection profiles. The protection profile provides the principal vehicle for customer-defined security requirements for IT products to include the specification of security features, development assurance, and evaluation assurance. The protection profile requirements for a particular class of IT products are described in the context of an assumed environment of use and set of generalized threats. The Federal Criteria builds on national and international IT product security research and development by bringing together and extending many concepts of previous work. While preserving the fundamental principles of IT product security, the Federal Criteria provides an extensible and flexible framework for defining new requirements as technology advances and the needs of the customer change. The criteria also provides the basis for international harmonization of IT product

security evaluation criteria, an important factor in motivating the development of cost-effective, commercial-off-the-shelf products by US vendors.

The OIW has a Special Interest Group (SIG) on OSI Security Architecture. The purpose of this group is to develop an overall OSI security architecture that is consistent with the OSI Reference Model and that economically satisfies the primary security needs of both the commercial and Government sectors. The SIG on OSI Security Architecture plans to address key management and security management functions that must be performed between the layers and the peer entities defined in the OSI architecture.

NIST Special Publication 800-4, *Computer Security Considerations in Federal Procurements* helps procurement initiators, contracting officers, and computer security officials understand the concepts for integrating computer security into agency acquisitions and for selecting needed computer security features, assurances, and procedures. [Ref. CSL 1992, 4]

11.2.4.3 ECMA Recommendations

In December 1989, ECMA issued a standard (ECMA 138) entitled *Security in Open Systems—Data Elements and Service Definition.* It is based on ECMA TR 46, *Security Framework* [Ref. ECMA 1988], which describes a framework for the development of security provisions in the Application Layer. ECMA 138 defines data elements and services for support of a multi-user, multi-vendor, distributed system environment.

While ECMA 138 addresses security in distributed systems, ISO 7498-2 addresses only communications security. Moreover, ECMA and ISO terminology are not consistent. ISO defines five security services and discusses them in terms of the mechanisms that may be used to implement the services and the layer of the ISO model where they may be appropriately implemented. ECMA defines eight different security services and eight security facilities they contain. However, the ECMA model deals primarily with two of the five services defined in ISO 7498-2: authentication and access control. [Ref. Burr 1991]

11.2.4.4 IEEE Work on Secure Local Area Networks (LANs)

IEEE is developing standards for secure LANs. The draft standards provide different service interfaces for key management, secure data exchange, and security management:

- IEEE P802.10A, *Interoperable LAN Security (SILS) - The Model*
- IEEE 802.10B, *SILS -Secure Data Exchange (SDE)*—a data link layer protocol providing confidentiality, integrity, data origin authentication, and access control services, 1992
- IEEE P802.10C, *SILS - Key Management, Draft, September 1993*—an application layer function that supports SDE by specifying a cryptographic key management model and protocol [Ref. IEEE SILS 1993]
- IEEE P802.10D, *SILS - Security Management*—an application layer set of services used to manage the security protocols.

Security management may be expanded to include fault, performance, and configuration management as well. In addition, IEEE P802.2 is considering an optional security sublayer for logical link control. [Ref. LLC 1988]

11.2.4.5 BLACKER

On the Defense Integrated Secure Network (DSNET), the Defense Information Systems Agency (DISA) operates a standard end-to-end encryption (E3) system called BLACKER. A

BLACKER front end (BFE) device is installed on each host-to-switch access path of all hosts used by subscribers, including terminal access controllers. The BLACKER system includes key distribution center (KDC) and access control center (ACC) hosts that automatically manage encryption keys via DSNET. BLACKER ensures that no network malfunction can permit or cause an unencrypted packet to be delivered to a host not authorized to receive it. [Ref. DCA 1990; Shirey n.d.; DCA 1989b]

BLACKER is designed to satisfy Class A1 of the DoD Trusted Computer System Evaluation Criteria (TCSEC), also known as "the Orange Book," by encrypting the application data in each X.25 packet while leaving header data unencrypted for backbone use. BLACKER makes DSNET multilevel secure in three ways. First, BLACKER separates subscriber security communities from each other, allowing the DSNET communities to share one backbone. Second, on the host side, the BFE recognizes a security label on each packet, allowing DSNET to serve a multilevel secure host through one BFE. Third, BLACKER separates the entire host community on one side of the BFEs from the backbone on the other, allowing the backbone to operate at a lower, less costly security level.

The host interface to the BFE is based on standards defined for the 1983 DDN X.25 interface, and requires that the Internet Protocol (IP) be used as the next layer above X.25. The BFE presents a Data Circuit-Terminating Equipment (DCE) interface to the host. Only DDN "Standard Service" X.25 is offered at the host interface; no provisions for "Basic Service" will be made. The BLACKER interface is, however, neither a pure X.25 interface nor a mere subset of X.25, but rather must be developed from X.25 interfaces.

The BFE conforms to the following Layer 3 specifications [Ref. DCA 1989b]:

- Defense Data Network X.25 Host Interface Specification, DCA, December 1983
- Interface Between Data Terminal Equipment (DTE) and Data Circuit Termination Equipment (DCE) for Terminals Operating in the Packet Mode on Public Data Networks, Recommendation X.25, ITU-TS, 1980
- WD2512 X.25 Packet Network Interface (LAPB), Western Digital Corporation, 1989.

In the Fall of 1989, a multi-Service demonstration that used BLACKER communications security and off-the-shelf gateways and routers was held in the United States. The Integrated Tactical-Strategic Demonstration Network (ITDN) used only non-developmental item components, standard data communications protocols (X.25 with TCP/IP), and existing military communications systems. ITDN interconnected automated systems at multiple echelons at widely dispersed (over 1,000 miles) locations with multiple-security-level interconnected networks.

Work similar to BLACKER is being done in other NATO nations to achieve the same ends.

11.2.4.6 Computer Security (COMPUSEC) Guidance

In order to guarantee secure handling of data and information technology systems, it is necessary to comply with security standards appropriate to the respective risks in differing operational environments. Commonly referenced security standards for COMPUSEC guidance are [Ref. CSC 1985; CSC 1985a; CSC 1985b; CSC 1987; ITSEC 1990]:

- *Computer Security Requirements—Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments* (Yellow Book), issued by the DoD Computer Security Center (DoDCSC) in June 1985
- *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements—Guidance for Applying the Department of Defense Trusted Computer System*

Evaluation Criteria in Specific Environments (Yellow Book Rationale), issued by DoDCSC in June 1985

- *Department of Defense Trusted Computer System Evaluation Criteria* (Orange Book), issued under the authority and in accordance with DoD Directive 5200.28 in December 1985. Its purpose is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of the overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems." The trusted computer system evaluation criteria classify systems into four broad hierarchical divisions of enhanced security protection: minimal, discretionary, mandatory, and verified.
- *Trusted Network Interpretation* (Red Book), issued by the National Computer Security Center in July 1987
- *Information Technology Security Evaluation Criteria (ITSEC)—Harmonised Criteria of France, Germany, The Netherlands, and the United Kingdom,* Draft, Version 1, May 1990.

11.2.4.7 ITU-TS Proposed Question on Security

ITU-TS Question Q19/VII, proposed for the 1993-96 study period concerns the continuation of work to date in security. While X.200 *(Reference Model of OSI for ITU-TS Applications)* and X.800 *(Security Architecture for Open Systems Interconnection for ITU-TS Applications)* describe security within the context of the open systems reference model, there is a need for a comprehensive set of more detailed frameworks covering aspects of security such as authentication, access control, confidentiality, etc., together with mechanisms, services, and protocols necessary to implement these models in both open systems in general and ITU-TS applications pertaining to the evolution of networks, systems, and services. Specifically, what new recommendations, if any, are needed:

- To describe open systems security frameworks?
- To describe open systems interconnection generic upper layers security facilities in the application and presentation layers?
- To describe information technology security techniques?
- To satisfy the security requirements of administrations and/or users who apply the open systems interconnection family of recommendations?

Moreover, what changes or enhancements should be made to Recommendation X.509 to correct deficiencies and/or better relate it to any new recommendations developed under this question? Finally, what changes or enhancements, if any, would be made to X.800? [Ref. SC21 N 6956 1992]

11.2.4.8 DoD Goal Security Architecture

The DoD Goal Security Architecture [DGSA, formerly the Defense-Wide Information Systems Security Program (DISSP) Goal Security Architecture] [Ref. DGSA 1993] establishes the conceptual target for all DoD information security architectures. It is integrated into the TAFIM, providing an integrated architectural focus, and providing guidance to security architects (i.e., it provides abstract architectural concepts of security to be embodied in specific information system architectures). A companion effort, the DGSA Overall Transition Strategy (DOTS), addresses the Defense-wide transition toward the incorporation of DGSA-specified security concepts into current and new information system architectures.

11.2.4.9 Kerberos

Kerberos is an authentication system for open systems and networks. Developed by project Athena at MIT, Kerberos can be added onto many existing network protocols. It has been used with UNIX-oriented protocols such as Sun's Network File System (NFS). Each user has a private authentication key. Kerberos guards the data transmitted between machines that communicate over the network and uses cryptographic keys known as tickets to protect the security of messages a user sends to the system (and the messages the system sends back to the user). It never transmits passwords, even in encrypted form, on the network. Passwords reside only in a highly secure machine called a key server. Kerberos performs authentication both when a user logs into the system and when the user requests any type of network service.

11.2.4.10 Secure Network File System

Sun Microsystem's Network File System (NFS has become a de facto standard for UNIX systems. NFS allows a client system to mount devices on a file server as if the server were physically connected to the system. Secure NFS uses two types of encryption: the data encryption standards (DES), a private key system) and a public key encryption system.

11.2.4.11 Multi-Level Security for Database Management

Government and industry are actively pursuing the development of multilevel security capabilities. In the context of database management, the term multilevel security (MLS) refers to the ability of a system to simultaneously process data of various sensitivities without risk of compromise. Mandatory access control (MAC), with which separation of sensitive data and access to that data is always automatically enforced, is the key component of multilevel secure systems. MAC provides a means of controlling access to data based on the sensitivity of the data, as represented by a label, and on the formal authorization or clearance of the user attempting to access the data. Each row of data within the database contains a label that represents the sensitivity of that row. In most MLS implementations, users can normally write information at a sensitivity label equal to their own sensitivity labels, and can read information at labels equal to or less sensitive than their own sensitivity labels.

Current examples of industry-led multilevel security development efforts are Trusted ORACLE7,[65] which is designed to meet Class B1, and ORACLE7, which is designed to meet Class C2 of the US Government's Trusted Computer System Evaluation Criteria (TCSEC; Orange Book). Trusted ORACLE7 is also designed to meet F-B1/E3 of the European Information Technology Security Evaluation Criteria (ITSEC). Trusted ORACLE7 is designed to be a full-function, open RDBMS; it adheres to standards such as ISO/ANSI SQL.

11.3 Assessment of Coverage by Standards

While there is a great deal of activity in standards for security services, there is very little that is complete. The most mature technical areas are operating system and physical layer network standards, but even here the standards are not mature. Security in most other aspects still contains areas of basic research. The standards that have been approved are generally the umbrella standards, such as ISO 7498-2.

---

[65] *Trusted ORACLE7 Technical Overview*, ORACLE Corporation, UNCLASSIFIED, January 1994.

12. SYSTEM MANAGEMENT SERVICE STANDARDS

This chapter summarizes the status of standards in four areas: network (OSI) management, registration authorities, conformance testing, and formal description techniques (FDTs). Appendix F identifies organizations and standards bodies that have contributed to development of these standards.

Standards for OSI management are described first (Section 12.1). These are followed by standards for conformance testing (Section 12.2) and registration authorities (Section 12.3). FDTs are addressed with conformance testing standards in Section 12.2.

Quick Reference	
Topic	Page
Assessment	293
CMIS/P	271
Conformance Testing	282
Estelle	289
FDTs	288
G-LOTOS	291
LOTOS	290
Managed Objects	263
Management SIGs	281
OSI Management	261
PICS Proformas	288
QoS	279
Registration Authorities	292
Structure of Mgmt Info	276
Systems Management	274
TMN	277
Z Description Language	291

12.1 Status of Standards for Network Management

This section discusses the status of OSI network management standards, the Telecommunications Management Network (TMN), military concerns in network management including quality of service (QoS) issues, the special interest groups (SIGs) for OSI management, the ECMA Model for Management, and the Simple Network Management Protocol (SNMP).

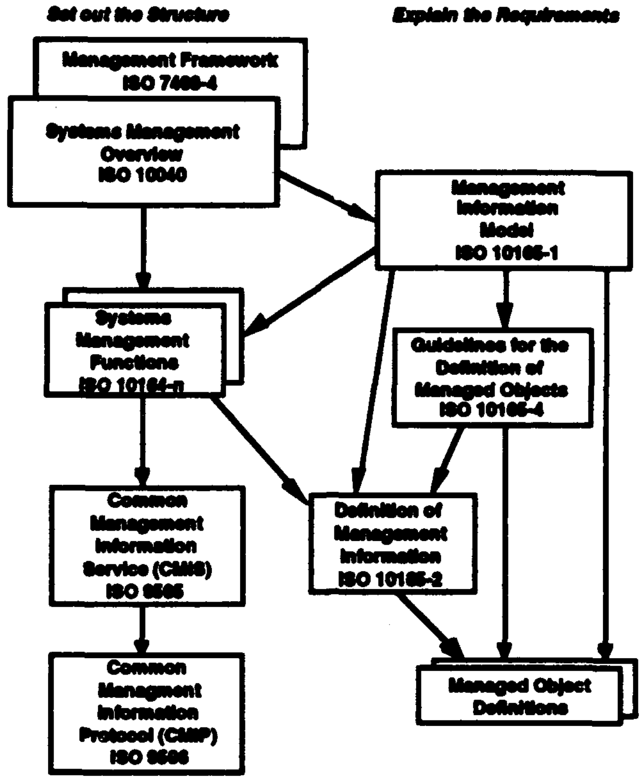
Part 4 of the OSI Reference Model, *Management Framework* (ISO 7498-4) identifies three areas of OSI management: systems management, layer management, and application process management. Development of international civil standards for the overall management architecture and for systems management is being coordinated through SC21/WG4 on OSI Management. The United States has developed a FIPS, (FIPS 179), *Government Network Management Profile (GNMP),* issued December 1992 based on this management framework. While a few products implement parts and subsets of the specification, NIST expects full implementations to be available in 1993. [Ref. APP 1992]

Figure 14 identifies the classes of OSI management standards and indicates the relationships among these classes. ISO standards are identified where they apply.

Work is progressing in SC6/WG2 and SC6/WG4 on OSI management in the lower layers. An international specification (ISO/IEC 10733) of the elements of network layer management information has been developed [SC6 N 6413, December 1990]. SC6 has developed a set of general principles for the definition of lower layer management [SC6 N 5784, January 1990; SC21 N 4630, April 1990]. These principles extend and refine the *Guidelines for the Definition of Managed Objects* (ISO 10165-4).

12.1.1 Development of OSI Management Standards

Network management standards are being developed by SC21/WG4. TSGCE SG9 activities have been directed at identifying issues and positions of concern to military applications and influencing the direction of the work in ISO/IEC. The emphasis of the TSGCE SG9 issues has been in the area of quality of service (QoS).



Source: ISO 10040, *Systems Management Overview*, SC21 N 6353, 4 September 1991. Updated October 1993.

Figure 14. OSI Management Standards

12.1.2 ISO Approach to OSI Management[66]

OSI Management concerns itself with three area: inter-system communications carrying management information, structure of the management information, and management functions to be undertaken by end systems. There are three ways by which management information is communicated:

- Systems Management protocols at the Application Layer
- Layer management protocols at lower layers
- Normal operation of layer protocols.

Systems Management is the preferred method. The others are required only because OSI Management concerns the resources and activities needed to monitor and control the open communications environment. They are not required for management outside OSI Management.

Systems Management uses a Common Management Information Protocol (CMIP) (ISO 9596) to communicate information between systems. This identifies information to be transferred and whether the transfer concerns an event report or an operation. Event reports are generated to notify another system of an asynchronous happening. Operations can monitor data

---

66 The discussion of the ISO approach to OSI management is taken from a working paper, *Open Distributed Management Standards--The OSI Management Approach*, A. Langsford (British Standards Institute IST21/P4 Chair), July 1989, UNCLASSIFIED.

and can exercise control either by assigning data values or initiating actions through a synchronous communication between end-systems.

12.1.2.1 Functional Areas

Establishing the scope of OSI Management is deemed necessary to establishing a consensus concerning the requirements. This led to identifying five functional areas for management: fault management, configuration management, accounting management, performance management, and security management. Although this approach had some advantages in resolving basic elements of functionality, it also exercised a constraining influence over the organization of work. Each functional area became concerned with its narrow perspective. This led to questions concerning the interplay between functional areas, exemplified by the following: "How does one handle standards for reconfiguring a system once a fault has been detected?"

12.1.2.2 Focus on Managed Objects

A clarification came from a shift of emphasis to the data of concern to management. Only when the data have been defined are the functions, which use the data throug' monitoring or controlling activities, considered. This has resulted in simpler functional standards. Each function can now stand alone rather than being bound into a composite document covering all the functions conceived as belonging to a particular area. It also enabled functions that cross the preconceived functional area boundaries to be handled in a natural manner. The result is that a particular function can be issued as a CD proposal when it is deemed to be technically stable without being unduly delayed by less mature work considered as belonging to the same functional area.

With this shift of emphasis towards data, the aim is now to identify the objects of concern to management, their attributes, and the operations that may be performed upon them. The communication services are thus the vehicles for carrying the values of attributes and a coded field identifying the operation to be carried out on a specific object, not for carrying information specifying a functional area. The approach is very close to (but not quite identical with) object-oriented methods. It has meant that work has concentrated on the management interchanges between systems performing a managing role and systems operating in an agent role manipulating internal managed objects. There has been little investigation of management exchanges between peer, managing entities, or of the management procedures invoked by managers.

The object-oriented approach has enabled OSI Management experts, in collaboration with those developing standards for various OSI layer protocols, to identify classes of managed objects and commonly used attributes. This in turn has promoted the development of a standard naming scheme through which to identify instances of object classes. The naming scheme is based on that used for Directory services. This facilitates the use of directories, conforming to ISO 9494 (ITU-TS Recommendation X.500), when management makes references to OSI objects.

A March 1991 paper entitled *Proliferation of Managed Objects* [SC21 N 5756] noted that many groups within ITU-TS and ISO are developing managed object definitions without the benefit of overall coordination. It suggests that this problem can only be solved by taking an overall view of managed object definition activities that requires a global management information authority, capable of influencing the activities of at least all the standards bodies.

Moreover, managed objects require garbage collection. Garbage collection comprises the garbage collector and the expiry behavior. The purpose of expiry behavior is to determine when an

object is subject to garbage collection. SC21/WG4 [SC21/WG4 N 1381] recently called for contributions on the definition of expiry behavior. [Ref. X3 1992b] The UK and Australian National Bodies see no need for special mechanisms to handle expiry behavior. A second WD *Working Document for Expiry Behaviour* [SC21 N 7959, July 1993] has been circulated to SC21 for study and comment; it was updated by SC21/WG4 in December 1993 [SC21/WG4 N 1831]. Expiry behavior is expected to be added to the scope of a new work item or to the Enhanced Event Control Function (WD 10164-ev) (see Section 12.1.3.1).

12.1.2.3 Distributed Processing Aspects

The shift of emphasis has been further beneficial in bringing into relief the fact that some management has been recognized as a distributed processing activity with its own managed objects. For example, the "event forwarding discriminator" takes management decisions about what should be done to asynchronous notifications flowing from OSI managed objects.

Thus, OSI Management standards are beginning to reveal explicitly what has always been known by management specialists; i.e., management is a distributed processing activity and has much in common with other distributed processing activities. Management's distinguishing feature is that the scope of the distributed application is limited to manipulating the information processing, storage, input/output, and communications environments themselves. Hence, particular attention is paid to controlling the permission to obtain and act upon system information.

SC21/WG4 requested national body contributions to progress a new work item on distributed management for discussion at a collaborative meeting held in the United Kingdom in December 1992. [Ref. SC21 N 7129 1992]

12.1.2.4 Results of Work in OSI Management

OSI Management has had a long learning process. The lessons learned have been valuable and appear to be applicable to management in general. The following steps are important in creating new management standards:

- Establish a requirement, since this sets the scope for the standard.
- Identify the objects of concern to management through which that requirement is realized. With identification of the objects goes the identification of their attributes, operations, and of any objects that can be encapsulated within the identified objects.
- Establish a naming scheme for the objects and their attributes.
- Identify management procedures that, through monitoring and controlling activities, meet the requirement. Where a procedure requires inter-system communication, the communication is provided through the use of CMIP.

The Structure of Management Information (SMI) standards for OSI set out rules for specifying managed objects, attributes, and their operations. Although detailed investigations remain to be carried out, first impressions are that these rules are applicable to all aspects of management. However, it could be that further investigation will reveal places where detail may need to be refined.

OSI Management standards identify a number of attributes that are common to many management activities (e.g., counters, gauges, thresholds, status, logs) and many events that have general applicability (e.g., fault reporting, exception handling). Though not yet as well developed, it appears that OSI management procedures for testing, accounting, managing, and accessing logs have the same general applicability. Adopting this work as a basis and providing extensions where

required will (a) obviate rework, (b) help limit the unnecessary proliferation of managed standards, and (c) help reduce the diversity of management software that suppliers have to write to support open distributed management.

In communicating related sets of operations to be performed or invoking remote operations, a managing system may wish to assert relative priorities to various tasks. If and how priority should be handled and communicated through CMIP is an open question.

12.1.2.5 Conformance

SC21/WG4 has only begun to describe how conformance statements should be constructed so that they apply meaningfully to OSI Management. The one exception is CMIP for which, being a conventional Application Layer protocol, the task of generating conformance statements is straightforward.

The main problem is that OSI Management is concerned not just with "how" something is communicated (CMIP) but "what" is communicated (SMI) and "why" (management functions and procedures). Whereas conformance and particularly the demonstration of conformance through conformance testing is readily applied to CMIP since the communication is visible and monitorable, the "what" and "why" require that conformance testing be applied to activities taking place within end systems. There is a need to investigate whether the approach of the OSI Conformance Testing Methodology is applicable or whether another method needs to be developed. Any method must recognize the distributed nature of management operations and so would probably be appropriate to other classes of distributed processing enterprise.

An April 1992 contribution on the testability of managed objects [Ref. SC21/WG4 N 1438 1992] addressed some of these issues. Subsequently, a question (Q1/63.2) on Testability of Managed Objects was registered. A draft answer (SC21 N 7079) suggested that emphasis be given initially to managed objects in the sense of testing the access to managed objects via CMIP and System Management Functions in the context of Network Management Profiles. [Ref. SC21 N 7079 1992]

Consideration of conformance to management standards, with the wider scope of open distributed processing, could have the beneficial effect of clarifying the conformance requirements, conformance clauses, PICS proformas (or the equivalent), and profiles for OSI Management standards. [Ref. Langsford 1989]

12.1.2.6 Security

SC21 N 6037, May 1991, called for contributions on the need for security services within OSI management. It identified the following security services:

- Access control
- Authentication (e.g., peer authentication, data-origin authentication)
- Integrity
- Auditing
- Confidentiality
- Non-repudiation.

The United Kingdom, in its response [SC21/WG4 N 1420], stated that of these services, only the audit functions were truly specific to WG4 and that WG4 need not specify its own functions for the other security services. It proposed specifying requirements and, in liaison with WG1 and WG6, ascertaining whether these requirements can be satisfied by other existing or

emerging standards. Canada, in its response [SC21/WG4 N 1433], concurred with the United Kingdom and proposed that WG4 prepare a security requirements statement and establish liaison with SC6 and SC21/WG6. The United States, in its response [SC21/WG4 N 1486], also agreed that management of security services should be an integral part of the development of security services and suggested assigning priorities to threats for the purpose of scheduling the development of security services.

As a result, in May 1992, SC21/WG4 issued a liaison statement to SC21/WG1, SC21/WG6, SC6, and SC27 on the security requirements of OSI systems management. It listed 11 requirements, of which it classified the following as high priority: authentication, access control, and auditing and alarm reporting. It further noted that alarm reporting, security audit trail reporting, and access control are already international standards (ISO/IEC 10164-7, 10164-8, and 10164-9, respectively; see Section 12.1.3.1 below). Thus, mature and stable work to satisfy these requirements are already available. WG4 requested comments on whether [Ref. SC21 N 7145 1992]:

- There are current developments that satisfy some or all of the requirements.
- The priorities are reasonable and in line with current work activities.
- Closer liaison to describe these requirements is desirable or necessary.

12.1.3 ISO Standards for OSI Management

A recent survey by the research company International Data Corporation (IDC) concluded that while users are cautious about actually migrating to OSI network management, they require suppliers to commit to providing it in the future. Moreover, OSI management has emerged as a possible solution to users' connectivity requirements. Finally, international networks are more focused on OSI management while in the United States the Simple Network Management Protocol (SNMP) (see Section 12.1.9) now evolving to SMP, has gained momentum as the management protocol of choice despite its limited functionality. [Ref. OSN 1992d]

Section 12.1.3.1 identifies the key OSI management standards and summarizes their status. The remaining parts of Section 12.1.3 expand on the work of SC21 on these and related standards projects.

12.1.3.1 Identification and Status of OSI Management Standards

Framework and Overview. The following give the overview and architecture developed for OSI management standards:

- *OSI Management Framework*, ISO 7498-4, November 1989 (ITU-TS X.700). The Framework document provides an architectural overview. In June 1993, SC21 proposed confirmation of this standard with addition of a technical corrigendum based on the January 1992 defect report [SC21 N 6658].
- *Systems Management Overview*, ISO 10040, November 1992 (ITU-TS X.701). The *Overview* document provides more detailed architectural concepts. It defines the architecture for systems management, which is management using Application Layer protocols for communication, and it sets out the scope of the other systems management standards.
    - AM 1, *Management Knowledge Management Architecture*, February 1993 [SC21 N 7527]
    - PDAM 2, *Management Domains Architecture*, November 1993 [SC21 N 7946] (balloting ended February 1994; editing meeting April 1994)

- Additional amendment or technical corrigendum to address changes to system management standards based on the final answer to Q1/49.9 on long-term solution to general and dependent conformance.

Systems Management Functional Areas (SMFAs). ISO/IEC 10164, *Open Systems Interconnection - Systems Management,* has been developed to address system management functions. Nearly 20 formal standards have been developed so far for *Systems Management.* Each is subject to a technical corrigendum resulting from the interim WG4 meeting in December 1993 and based on SC21 N 7966, which incorporated the final answer to Q1/49.9 on the long-term solution to general and dependent conformance. Amendments entitled *ICS Proforma* were originally entitled *MOCS/PICS Proforma.* The first seven of these amendments are expected to progress to IS status (AMs) following conclusion of balloting in June 1994 and the editing meeting of July 1994; initiation of ITU-TS approval expected November 1994. The parts of *Systems Management* and their amendments are as follows:

- ISO/IEC 10164-1 (Part 1): *Object Management Function,* June 1993 (X.730)
  - DAM 1, *ICS Proforma,* December 1993 [SC21 N 8240]
- ISO/IEC 10164-2 (Part 2): *State Management Function (ITU-*TS X.731)
  - DAM 1, *ICS Proforma,* December 1993 [SC21 N 8241]
- ISO/IEC 10164-3 (Part 3): *Attributes for Representing Relationships* (X.732)
  - DAM 1, *ICS Proforma,* December 1993 [SC21 N 8242]
- ISO/IEC 10164-4 (Part 4): *Alarm Reporting Function,* December 1992 (X.733)
  - DAM 1, *ICS Proforma,* December 1993 [SC21 N 8243]
- ISO/IEC 10164-5 (Part 5): *Event Report Management Function,* June 1993 (formerly entitled *Management Service Control Function)* (X.734)
  - DAM 1, *ICS Proforma,* December 1993 [SC21 N 8244]
  - PDAM 2, *Enhanced Discriminator,* August 1993 (editing meeting April 1994)
- ISO/IEC 10164-6 (Part 6): *Log Control Function,* November 1993 (X.735)
  - DAM 1, *ICS Proforma,* December 1993 [SC21 N 8245]
  - PDAM 2, *Enhanced Log,* August 1993 (editing meeting April 1994)
- ISO/IEC 10164-7 (Part 7): *Security Alarm Reporting Function,* May 1992 (X.736)
  - DAM 1, *ICS Proforma,* December 1993 [SC21 N 8246]
- ISO/IEC 10164-8 (Part 8): *Security Audit Trail Function,* June 1993 (X.740)
- ISO/IEC 10164-9 (Part 9): *Objects and Attributes for Access Control,* November 1993 [SC21 N 7661] (X.741) (ballot ended October 1993; editing meeting February 1994; initiation of ITU-TS approval expected February 1994)
- DIS 10164-10.2 (Part 10): *Usage Metering Function,* November 1993 (formerly entitled Accounting Meter Function) [SC21 N 8238] (X.742) (ballot ended February 1994; editing meeting April 1994; initiation of ITU-TS approval expected November 1994)
  - WDAM 1, *ICS Proforma,* September 1993 (PDAM expected July 1994)
- ISO/IEC 10164-11 (Part 11): *Metric Objects and Attributes,* March 1993 (formerly entitled Workload Monitoring Function) (X.739).
  - WDAM 1, *ICS Proforma,* September 1993 [SC21 N 8162] (PDAM expected July 1994)
  - WDAM 2, *Additional Metric Objects and Attributes,* September 1993 [SC21 N 8161] (PDAM expected July 1994)
- ISO/IEC 10164-12 (Part 12): *Test Management Function,* December 1992 (X.745)
  - PDAM 1, *ICS Proforma,* November 1993 [SC21 N 8335]

- ISO/IEC 10164-13 (Part 13): *Summarization Function*, September 1993 (X.738)
  - WDAM 1, *ICS Proforma*, September 1993 [SC21 N 8163]
  - WDAM 2, *Additional Summarization Scanners*, July 1993 [SC21 N 7963]
- DIS 10164-14.2 (Part 14): *Confidence and Diagnostic Test Categories*, May 1993 [SC21 N 7454] (X.737)
- ISO/IEC 10164-15 (Part 15): *Scheduling Function*, April 1993 [SC21 N 7683] (editing meeting February 1994; initiation of ITU-TS approval expected November 1994) (X.746)
- CD 10164-16.2 (Part 16): *Management Knowledge Management Function*, October 1993 [SC21 N 8310] (initiation of ITU-TS approval expected November 1994) (X.750)
- CD 10164-17 (Part 17): *Change Over Function*, January 1994 [SC21 N 8422] (note that the Change Over Function is similar to, and possibly a generalization of, the Synchronous Data Hierarchy Protection Switching Function developed by ITU-TS SG15) (initiation of ITU-TS approval ballot expected in 1997) (X.751)
- CD 10164-19 (Part 19): *Management Domain and Management Policy Management Function*, January 1994 [SC21 N 8423] (initiation of ITU-TS approval ballot expected in 1997) (X.749)

Work in SC21/WG4 on OSI management is continuing on several new parts for *Systems Management*, ISO 10164. CDs are expected in 1994; initiation of ITU-TS approval expected in 1997.

- WD 10164-cs: *Command Sequencer for Systems Management*, December 1993 [SC21 N 7962; SC21/WG4 N 1832]]
- WD 10164-ev.2: *Enhanced Event Control Function*, second WD, July 1993 [SC21 N 7958]. This NWI passed in May 1992 and Expiry Behavior (see Section 12.1.2.2) was added to its scope. [Ref. SC21 N 7107 rev 1992]
- WD 10164-rm.2: *General Relationship Management Function*, second WD, June 1993 [SC21 N 8040]
- WD 10164-rtm: *Response Time Monitoring Function*, August 1990 [SC21 N 7970; JTC1 N 963]
- WD 10164-sw: *Software Management Function*, September 1993 [SC21 N 8201]
- WD 10164-tm.2: *Time Management: Function Representation of Time*, second WD, July 1993 [SC21 N 7961]—deals with the distribution and synchronization of time in a distributed environment.

Profiles. The three regional workshops (AOW, EWOS, and OIW) are currently developing profiles (DISP 12059-2, Annex B) for use of *Systems Management* standards (ISO/IEC 10164-1 to -6) and the Definition of Management Information standard (ISO 10165-2). [Ref. SC21 N 6915 1992]

Liaison and Coordination. Noting overlap between the scope of work within SC21/WG4 and SC22/WG15 (System Administration Interface/Software), JTC1, and the ITU-TS Software Management Subgroup established at a Collaborative Meeting on Systems Management in November 1991, that SC21/WG4 should be concerned only with the management aspects of software resources, and that SC22/WG15 should be concerned with wider aspects such as portability, packaging, distribution, administration, and management aspects. JTC1 and the ITU-TS Software Management Group requested that an official liaison be established between the two working groups to consider this issue and agree on a common position for future work and

collaboration. [Ref. SC21 N 6664 1992] The work of WG4, originating from the IEEE P1003.7b Software Management project (see Section 10.2.1.1) and WG4's *Software Management Function* (WD 10164-sw) are on roughly comparable schedules. The two groups plan to continue cooperating by exchange of future drafts, with liaison continuing as the opportunity arises. [Ref. SC21 N 7146 1992]

There is also substantial overlap between WD 10164-tm, *Time Management Function* [SC21 N 7961], and the SC18/WG4 proposed *Coordinated Time Service* standard (see Section 9.13.1).

Structure of Management Information (SMI). ISO/IEC 10165, *Structure of Management Information*, has the following parts (Part 3 was cancelled in November 1989 by recommendation of SC21 and incorporated into Part 2):

- ISO/IEC 10165-1 (Part 1): *Management Information Model*, September 1993 (X.720)
  - PDAM 1: *Generalization of Terms*, June 1993 [SC21 N 7847] (formerly entitled *General Relationship Model;* editing meeting February 1994)
- ISO/IEC 10165-2 (Part 2): *Definition of Management Information*, July 1993 (X.721)
  - PDAM 1.2, *Enhanced Discriminator and* Log, January 1993 [SC21 N 7559]
- ISO/IEC 10165-4 (Part 4): *Guidelines for the Definition of Managed Objects*, September 1992 (X.722)
  - PDAM 1, *GDMO Extensions*, July 1993 [SC21 N 7948] (formerly entitled *General Relationship Model)*
  - PDAM 2, *Set By Create and Component Registration*, 1993 (editing meeting February 1994)
- ISO/IEC 10165-5 (Part 5): *Generic Management Information*, March 1993 (X.734) (previously entitled *Generic Managed Objects)*
- ISO/IEC 10165-6 (Part 6): *Requirements and Guidelines for Implementation Conformance Statement Proformas Associated with Management Information*, June 1993 [SC21 N 7894] (X.724)
  - WDAM 1, *Manager Role Conformance* [SC21 N 7964, July 1993]
- CD 10165-7.2 (Part 7): *General Relationship Model*, September 1993 [SC21 N 8036] (X.725) (formerly entitled *Management Information Register (MIR) and Registration Procedure).*

Management Information in the Upper Layers. A WD has been developed on *Managed Objects in the Upper Layers*, June 1993 [SC21 N 8178]. Work on this document was transferred in June 1993 from SC21/WG8 to SC21/WG4. CD status is expected July 1994. The document establishes a model for common upper layer objects, gives an overview of the definitions imported from the *Generic Management Information* (ISO/IEC 10165-5), and provides generic and formal definitions for common upper layer information (managed objects). The model for managed objects includes a naming tree, basic building blocks, extended application layer structure (XALS) recursive model, provision for separable upper layers, and provision for a monolithic upper layer entity.

System Management Communications. Standards have been defined to specify services and protocols for exchanging management information. They are the collaborative effort of ISO/IEC and ITU-TS. The system management communications standards are the following:

- ISO/IEC 9595:1991, *Common Management Information Service (CMIS) Definition*, Edition 2 (incorporates AM 1 and AM 2), April 1991 (X.710). CMIS defines services for acting on an object and includes creation and deletion. Services can apply

to values from a set of attribute values; the attribute values can have the structure of a table, so that services can affect entries, entire rows, and entire columns. Amendments are the following:

- PDAM 3, *Support of Allomorphism,*[67] November 1990—project was cancelled by JTC1 on the recommendation of SC21 in May 1992
- AM 4, *Access Control,* July 1992—addresses the use of the access control field
- WDAM 5, *Enhanced Functionality for System Management Communications,* June 1993 [SC21 N 7970]; PDAM expected December 1994.

- ISO/IEC 9596-1:1991, *Common Management Information Protocol (CMIP),* Part 1: *Specification,* Edition 2 (incorporates AM 1 and AM 2), June 1991 (X.711). CMIP defines peer protocols for layer services between Systems Management entities. Amendments are the following:
  - PDAM 3, *Support of Allomorphism,* July 1990—project was cancelled by JTC1 on the recommendation of SC21 in May 1992
  - PDAM 4, *State Tables for CMIP,* January 1990 [SC21 N 4058]—project cancelled June 1991).
  - WDAM 5, *Enhanced Functionality,* June 1993 [SC21 N 7970], PDAM expected December 1994.
- ISO/IEC 9596-2:1991, *Common Management Information Protocol (CMIP),* Part 2: *PICS Proforma,* June 1993 (X.712).

Other OSI Management Standards. Other OSI management standards are as follows:

- ISO/IEC 10733, *Telecommunications and Information Exchange Between Systems - Elements of Management Information Related to OSI Network Layer Standards,* 1993.
- ISO/IEC 10737, *Specification of the Elements of Management Information Related to OSI Transport Layer Standards,* 1993. A liaison statement from SC6/WG4 to the ULA group cited ISO/IEC 10737 as an example of a layer management specification. SC6/WG4's examination of ISO/IEC 10737 discovered two problems with the managed-object structure described in the document that seem to contradict the Reference Model. [Ref. SC21 N 6606 1991]
- CD 11587.2, *Application Context for Systems Management with TP,* July 1993 [SC21 N 7899] (editing meeting February 1994; initiation of ITU-TS approval expected June 1995) (X.702)

Management Issues. In response to a request for NB comments on the progression of an Amendment to ISO 10164-11 on the Definition of Multiple Input Metric Objects, the United States submitted a document on a *Method for Comparing Counters to Set Threshold Levels for Generating Notifications.* If accepted, the United States intends to provide further enhancements that will provide further basis for the amendment. [Ref. SC21 WG4 N 1472 1991] A Preliminary Document on Multiple Input Metric Objects [SC21 N 7134] was proposed in May 1992. The Performance Management Group proposes progressing it as an amendment to the workload monitoring function (ISO 10164-11). [Ref. SC21 N 7134 1992] The items to be considered for this addendum include:

- A Metric Managed Object (or set of metric objects) that would provide the identifier of the algorithm used to calculate the metric

[67] An object in a refined class (i.e., a subclass) of a class definition (e.g., a modem) could behave in certain situations as if it were the parent. This characteristic, called polymorphism or more recently allomorphism, would support backwards compatibility. The way in which an object would respond would depend on how it is addressed.

- A set of Multiple Input Metric Object Classes
- A new algorithm for the calculation of percentiles (Exponentially Weighted Stochastic Approximation (EWSA)) that will provide a higher degree of accuracy at the tails of the distribution than the EWMA percentile algorithm currently defined in 10164-11.

The December 1992 editing meeting also agreed that the ICS for ISO 10164-11 should be progressed as an addendum, but separately from the items listed above. [Ref. SC21 N 7535 1993] The ICS requirements for 10164-11 are detailed in [Ref. SC21 N 7534 1993].

One of the major issues raised at the *Test Management Function* (ISO 10164-12) editing meeting in October 1991 was a proposal to incorporate the concept that a managing system may request that a test be run with a given priority. The requirement was accepted, but it was considered by the majority of the meeting that prioritization was a general requirement and should be progressed as such. The editing group requested that the Common Management Working Group consider prioritization as a work item. [Ref. SC21 N 6559 1991]

In support of the Telecommunication Management Network (TMN) development (see Section 12.1.4), ITU-TS SG XI is developing a model for performance monitoring to be documented in Draft Recommendation Q.82pm, *Stage 2 and Stage 3 Description for the Q3 Interface - Performance Management*. This model uses the functionality defined in ISO 10164-13 for the object classes Scanner, homogeneous Scanner, Simple Scanner, and scanReportRecord. Thus, ITU-TS recommends keeping this functionality as currently documented in ISO 10164-13. In addition, they would like to add to the behavior of the Scanner object class the capability to scan itself. [Ref. SC21 N 6896 1992]

In November 1990, it was agreed that after Version 2 of CMIS and CMIP there will be no further releases (either in the form of addenda or completed standards) that could affect interoperability before 1994 [Ref. SC21 N 5546 1990]. Therefore, in nominating solutions for the NWI on *Enhanced Functionality for Systems Management Communications*, National Bodies were asked to consider solutions that do not require enhancements to CMIS/CMIP.

In a liaison statement to SC21/WG4, ITU-TS SG VII state that the enhancement to CMIS/CMIP (see Section 12.1.3.2) on transaction processing capability for ITU-TS applications is an important work item in the next study period in ITU-TS SG VII Q.24. An attached document brings up several requirements that could be satisfied by new work on atomic transaction support. [Ref. SC21 N 6892 1992]

Moreover, in a joint meeting of WG1 and WG4 of SC21 on the Draft Technical Corrigendum (TC) to ISO 9596-1 in Ottawa in May 1992, it was agreed to deprecate the use of the concept of general and dependent conformances; due to incompleteness of its development. Thus, the Draft TC was amended so that the concept of general and dependent conformance classes was removed and replaced by concise statements concerning what claims to conform to CMIP may be made. The revised text was submitted to the ISO Central Secretariat for publication. However, ITU-TS SG VII disagrees and believes the concept of dependent conformance (i.e., allowing referencing standards to use a subset of CMIS services, and to have their conformance claims requiring conformance only to the relevant CMIP protocol elements associated with the services used) is stable and plans to publish its approved text without those changes. [Ref. SC21 N 6894 1992] In May 1992 WG1 proposed a new subquestion (Q1/49.9) on long-term solution to general and dependent conformance. The draft answer [Ref. SC21 N 7069 1992] states that the concept of general conformance is misleading and should be avoided. Moreover, the concept of dependent

conformance is not needed, since it was introduced to contrast with general conformance. Therefore, conformance to a protocol should be expressed without use of either term. A final answer was expected in May 1993. [Ref. SC21 N 7073 1992] PDAMs to SM Overview (ISO 10040) and the SM Function standards (ISO 10164) on General and Dependent Conformance are expected in December 1993.

12.1.3.2 New Work Items

New work items include:

- *Systems Management Tutorial*, May 1992 [SC21/WG4 N 1532] (planned to be a new technical report) (ITU-TS X.702). Second WD. CD provisionally expected December 1993. Several issues still need to be resolved, however. For example, agreement is needed as to the target audience and purpose. The *SC21 Programme of Work* [SC21 N 7205, September 1992] requested JTC1 endorsement to cancel the project.
- *Extended Systems Management Architecture*, July 1993 [SC21 N 7957] describes the requirements for the extended systems management architecture. It is for further study whether this will be a separate standard (that might replace the current Systems Management Overview), or this will be an addendum to the current Systems Management Overview (ISO 10040) At the Collaborative Meeting of ITU-TS Q24/VII and ISO/IEC JTC1/SC21 WG4 SM Rapporteur Groups in December 1992, it was decided to use a WG4 Standing Document as a vehicle to maintain a list of issues for Extended Systems Management Architecture. The issues in the current SD (WG4 SD1) [Ref. SC21 WG4 N 1641 1992] are:
  - Communication support for distribution
  - Naming in the Extended Systems Management Architecture
  - Scoping and filtering in multi-system environment
  - Recursive domains
  - Visibility of managed objects
  - Naming schema objects
  - Definition of managed objects for systems management protocol machines. A WD *Definition of System Management Protocol Machine Managed Objects* [SC21 N 7965] was produced in September 1993.
- *Formal Descriptions of CMIP*, July 1990 [SC21 N 4947].
- *Managed Object Conformance Statement (MOCS) Proformas*, February 1991 [SC21 N 5686]—to provide requirements and develop a standard specification technique (template) for MOCS proforma, thus helping to ensure their completeness, consistency, and ease of use. MOCS proformas are analogous to PICS proformas, but apply to managed object definitions as opposed to protocols.
- *Management Information for the OSI Upper Layers* [SC21 N 4108] (approved by JTC1 in May 1990). In May 1991, SC21/WG6 issued a request for comment on requirements for this NWI [Ref. SC21 N 6067 1991]. Only the United States responded, and, while the ULA group felt that the response [SC21 N 6799] represented good initial work on the topic and posed interesting questions, it also felt that this work cannot be progressed without more NB participation. Accordingly, it urgently requested comments on the US contribution [Ref. SC21 N 6968 1992]. Some issues that the US contribution highlighted include:
  - Defining recursion through relationship attributes in managed objects for XALS to correspond with the recursion of XALS objects
  - Identifying advantages and disadvantages of alternative definitions of managed object classes to represent the resources in the upper layers

- Using the management domain concept to differentiate between managed objects for different applications
- Distinguishing between application management vs. application layer management
- Clarifying what is meant by information for "autonomous management of the open system" in ISO 7498-4 as information that is stored in the management information base.

This project has been transferred from WG 8 to WG 4. A related document, *Working Document on Managed Objects for Upper Layers,* is SC21 N 8178, dated August 1993.

In April 1992, SC18/WG4 circulated a proposal for a NWI on *Mapping of the OSI System Management - Object Management Function onto Message Oriented Text Interchange System (MOTIS).* The work is to define a new standard in order to enable management information to be carried over MOTIS. In addition, an addendum to ISO 10164-1 would be produced. Annexes B (*MHS Model*), C (*Mapping Between PT-Service and MHS MTS-Service*), and D (*X-Protocol Specification*) of ITU-TS Draft Recommendation X.cnms, *Definition of Customer Network Management Services for Public Data Networks*, are also relevant. WD status was expected in June 1993, CD in November 1993, DIS in June 1994, and IS in June 1995. [Ref. SC21 N 7483 1992]

A Collaborative Meeting of ITU-TS Q24/VII and ISO/IEC JTC1/SC21 WG4 SM Rapporteur Groups in December 1992 made the following recommendations [Ref. SC21 WG4 N 1615 1992]:

- That a standard for managed objects for the application layer be developed
- That an Implementor's Guide be produced and maintained to record defect progress and resulting textual changes to standards.

After reviewing the NB comments on a call for comments on requirements for support for complex attribute types, the SMI Rapporteur Group concluded that a requirement had been established for the support of set-valued attributes to model table structures. Accordingly, WG4 produced a *Working Document on Complex Attribute Types*. [SC21 N 7116, July 1992] However, Australia contends that complex attributes can be represented using the current OSI information modelling tools. [Ref. SC21 N 7116 1992]

An NP for *Command Sequencer for Systems Management* [JTC1 N 2246] has been accepted into the JTC 1 program of work, but SC21 has been requested to respond to comments received. SC21 N 7962, dated July 1993 is the Working Draft for this new work item. As noted, it is expected to become a new part of ISO/IEC 10164.

The general requirements of a NWI entitled, *Enhanced Functionality for Systems Management Communications* are [Ref. SC21 N 7728 1993]:

- Bulk data transfer
- Complex attributes
- Management associations - quality of service
- Object selection
- Synchronization
- Protocol operational behavior
- Deadlocks.

The WD is SC21 N 7970. Target dates for the project were CD in May 1993, DIS in December 1993, and IS in August 1994. [Ref. SC21 N 7105 1992]

WG4 has proposed several new work items that have not yet been officially assigned [Ref. SC21 N 7630 1993]:

- *CMIP Machine Managed Object* [SC21/WG4 N 1643]
- *Management Information Model Extension* [SC21/WG4 N 1633; SC21/WG4 N 1638]
- *Manager Role Conformance*, December 1993 [SC21/WG4 N 1853]
- *Extended Scanners* [SC21 N 7134; S21 N 7223]
- *Management Information Library* [SC21 N 7132].

SC21/WG4 has develop a document, *Requirements and Directions for the Use of Formal Description Techniques for the Specification of Managed Objects*, October 1993 [SC21 N 8280]. The document addresses the need to use formal techniques rather than plain language descriptions, model-based approaches, object-oriented paradigm, life-cycle requirements, migration, and possible replacement (as a long-term goal) of the GDMO with an alternative FDT. Review of FDTs focuses on SDL and Z, with some preference for SDL.

SC21/WG4 has a standing document (SD-1) on *Issues for Extended Systems Management Architecture*, July 1993 [SC21 N 7955 Revised], which identifies issues to be relevant for the extended architecture for systems management. ITU-TS SG7 has issued and maintains the *OSI Systems Management Implementors Guide*, Version 1, July 1993 [SC21 N 8281], which records known defects in network management standards: ITU-T X.700-Series Recommendations, ISO/IEC 9595, 9596, 10040, 10164, and 10165.

12.1.3.3 Systems Management, ISO 10164

Standards. ISO 10164, *Systems Management*, establishes user requirements for each management function, establishes a model that relates the services and generic definitions provided by this function to user requirements, defines the services provided, defines generic notification types and parameters documented in accordance with the guidelines for the definition of managed objects, specifies the protocol necessary to provide the service, specifies the abstract syntax necessary to identify and negotiate the functional units in the protocol (if necessary), defines the relationship between the services and systems management operations and notifications, specifies compliance requirements placed on other standards that make use of these generic definitions, defines relationships with other systems management functions, and specifies conformance requirements. ISO 10164 does not define implementation aspects, specify the manner in which management is accomplished, define interactions that result in the use of management functions, specify services for establishment and normal or abnormal release of a management association, or define managed objects. The major management functions addressed in systems management are defined in Table 36.

ISO 10164 defines particular systems management functions and how these are achieved by use of CMIS ASN.1 is the notation used to express the abstract syntax of the data elements associated with managed object, attribute, event, and action definitions that shall be carried in CMIP.

Issues. The following technical issues are not yet addressed by ISO 10164 [Ref. SC21/WG4 1989]:

- Renaming managed objects—requirements for renaming managed objects, including classes to be renamed, conditions under which rename would be permitted, constraints on renaming objects in standardized procedures, and changes that need to be coordinated to make a renaming operation consistent and meaningful.

- Service access control—mechanism to address the need for individual open systems to have the option of protecting themselves against the invocation of services that would forcibly change existing configured relationships among managed objects.
- Startup and shutdown—addressing the requirement to manage the state of an object as regards invoking startup (or initialization) and shutdown.

Table 36. Definitions of OSI Systems Management Functions

• <u>Access control</u>—provides consistent levels of granularity necessary to a homogeneous control policy, preventing management notifications from being sent to unauthorized recipients, preventing initiators from having access to management operations, and protecting management information from unintended disclosure. Various levels of access control will be supported: some users may be given read and write access to specific attributes while other users have only read access or no access; some users may be granted access only to specific managed objects; and some users may not be allowed to establish management communications at all.
• <u>Alarm reporting function</u>—reports alarms, errors, and related information. Malfunctions will range in severity from minor, where a minimal impact upon the quality of service to the user occurs, to major, where it is no longer possible to provide the quality of service requested (or promised to) the service user.
• <u>Event report management</u>—the ability to specify conditions to be satisfied by a potential event report relating to a particular managed object or a set of managed objects, in order to be sent to specified destinations.
• <u>Log control</u>—the ability to preserve information about events that may have occurred or operations that may have been performed by or on various objects.
• <u>Object management</u>—ability to create, delete, examine, and change sets of management information that describe parts of the OSI environment.
• <u>Relationship management</u>—the ability to examine the relationships among various parts of the system, to see how the operation of one part of the system depends upon is depended upon by other parts.
• <u>Security alarm reporting function</u>—provides such capabilities as the means to receive notifications of security-related events, alerts of any misoperations in security services and mechanisms, alerts of attacks on system security, and information as to the perceived severity of any misoperation, attack, or breach of security. The standard provides notifications that include reporting of the clearance of fault conditions.
• <u>Security audit trail</u>—the ability to maintain a record of security-related events that occur in the management domain and to review and analyze these events to detect security breaches, malfunctions, and effectiveness of the security services and mechanisms that are implemented pursuant to the security policy.
• <u>State management</u>—the ability to examine and be notified of changes in state, to monitor overall operability and usage of objects in a consistent manner, and to give or withhold permission for the use of specific objects.
• <u>Summarization function</u>—measures throughput, time delays, message round trips, response times, and other measures of congestion and resource utilization for performance monitoring and statistics calculated across managed objects, not over time (see Workload Monitoring Function).
• <u>Test management function</u>—remote control of tests involving real open systems and the specification of tests that exercise OSI resources.
• <u>Workload monitoring function</u>—may be used by an application process in a centralized or decentralized management environment to interact to satisfy such requirements as: - Definition of statistical monitoring tools to derive metrics to characterize performance - Definition of a monitoring function that provides metrics of the workload, workload rejected, and resources used - Specification of mechanisms to obtain these metrics - Specification of notifications to be generated when these metrics exceed threshold values, and the ability to include additional performance information into these notifications - Specification of mechanisms to control the operation of this function, for example to initiate and to terminate monitoring - Scheduling of metric monitoring over a specified period of time.

Source: ISO 10164-1, June 1993.

Specific concerns regarding ISO/IEC 10164-9, *Objects and Attributes for Access Control*, are that the document is technically flawed, the technology in the document is already obsolete, and the document contents are inconsistent with its scope. Moreover, Part 9 needs alignment with the *Access Control Framework*, DIS 10181-3. [Ref. X3 1991j]

A working draft on Change Over Function was prepared in June 1992. It defines services for managing backup relationships and specifies a set of associated generic definitions. Liaison between SC21/WG4 and ITU-TS SG15 has been initiated to determine the possible overlap of the Change Over Function and the Synchronous Data Hierarchy (SDH) protection switching model. [Ref. SC21 N 7980 1993]

12.1.3.4 Structure of Management Information (SMI) (ISO 10165)

The Structure of Management Information (SMI) now has seven parts. The purpose of ISO 10165-1, *Management Information Model*, is to give structure to the management information conveyed externally by systems management protocols and to model management aspects of the related resources (e.g., an X.25 protocol machine). Managed objects are abstractions of data processing and data communications resources (e.g., protocol state machines, connections, modems) for the purposed of management. It is the attributes, operations, and notifications of managed objects that are visible to management, whereas the internal functioning of the managed object (i.e., the resource it represents) is not otherwise visible to management. ISO 10165-1 describes the model of management information in terms of managed objects and the set of operations that may be performed upon them and notifications that they may generate. It also defines, using object-oriented principles, key concepts such as inheritance, allomorphism, containment, and naming as they relate to managed objects.

ISO 10165-2 defines the generic object classes, support managed object classes, abstract attribute types, attributes types, notifications types, action types, parameter types, and associated abstract syntaxes that may be applicable to a number of different standards. It also specifies compliance requirements placed on other standards that make use of these definitions.

ISO 10165-4 defines the management information that is to be transferred or manipulated by means of the OSI management protocol and the managed objects to which that information relates. ISO 10165-4 provides developers of managed object class definitions with the information and documentation tools that are required in order to produce complete managed object class definitions. An amendment to this standard is being proposed to align it with 10165-1 by adding the ability to specify an explicit value for individual attributes. [Ref. SC21 WG4 N 1640 1992]

ISO 10165-5, *Generic Management Information*, provides developers of OSI specifications that contain managed object definitions with generic definitions of managed object classes that will:

- Provide common superclass definitions from which layer- or resource-specific object class definitions may be derived
- Assist with the development of common elements of object class definitions across multiple layers or components of layers
- Reduce duplication of effort in other working groups by identifying commonly useful definitions.

In May 1992, at the SC21/WG4 SMI Rapporteur Group meeting, it was agreed to restrict the scope of ISO 10165-6, *Requirements and Guidelines for Implementation Conformance Statement (ICS) Proformas* to standards for management information. This decision effectively restricts management conformance proformas to apply to managed systems. In agreeing to this restriction, a number of NBs urged that attention be given to developing conformance proformas for managing systems. In July 1992, WG4 requested NB input on principles for conformance for managing systems. [Ref. SC21 N 7117 1992] NB contributions are contained in [Ref. SC21/WG1 N 1233 1993].

CD 10165-7.2, *General Relationship Model* (formerly entitled *Management Information Register (MIR)),* is in a second CD ballot as SC21 N 8036, September 1993.

In a liaison statement [Ref. SC21 N 7588 1993] to ITU-TS Q24/VII concerning Q24/VII's intention to choose a formal description technique (FDT) for the specification of managed-object behavior, the SMI Rapporteur Group of SC21/WG4 highlighted two related ISO activities:

- SC22 proposal to standardize the FDT Z [JTC1 N 2159]
- Work in the area of architectural semantics being progressed by SC21/WG7 and their comparison and analysis of various FDTs including LOTOS, ESTELLE, SDL, and Z (see Section 12.2.3).

12.1.3.5 OSI Management Profiles

The following are ISPs for OSI management (a complete list of all the parts is provided in Appendix E):

- DISP 12059, *Management Functions - Common Information for Management Functions* (Parts 0-6), 1992
- DISP 12060, *ISPs AOM nnn - OSI Management - Management Functions* (9 parts), 1992.

The EWOS Expert Group on Network Management (EG-NM) has developed *Guidelines for Managed Object Taxonomy and Profiles,* Draft 3, July 1993 [EWOS/TA/93/239]. The EWOS EG-NM has also developed a taxonomy for future profiles [SGFS N 1076; EWOS/TA/93/327], December 1993. A summary of this taxonomy is provided in Table 37.

12.1.4 Telecommunication Management Network (TMN)

The Telecommunication Management Network (TMN) is a concept developed by ITU-TS (Recommendation M.30) to manage a telecommunication network (e.g., the public telephone network or an ISDN). A TMN is conceptually a separate network that interfaces a telecommunications network at several different points to receive information from it and to control its operations. A TMN may use parts of the telecommunications network to provide for its own communications.

Architecturally, the TMN functions are divided into three blocks:

- Operation System Function (OSF) that processes the information related to telecommunication management to support or control the realization of various telecommunication management functions.
- Mediation Function (MF) that acts on information passing between Network Element Functions (see below) and OSFs to achieve smooth and efficient communication. The main MFs are communication control, protocol conversion, data handling, communication of primitives, processing involving decision making, and data storage.
- Data Communication Function (DCF) that provides the means to transport information related to telecommunication management between functional blocks.

The three functional blocks can communicate with two external blocks. One is the Network Element Function (NEF) that communicates with a TMN for the purpose of being monitored and/or controlled. The other is the Workstation Function (WSF) that provides the means for communications between function blocks (OSF, MF, DCF, and NEF) and the user. The current draft of the *NATO C3 Architecture Communications Subsystem* (July 1989) indicates that the management of the NATO ISDN (see Section 17.3.6) will be based on the TMN concept.

[Ref. Man 1990] The NATO Tactical Communications Architecture (see Section 18.1.3) proposed by TSGCE SG11/PG6 is also based on TMN.

Table 37. Proposed Taxonomy for OSI Management Profiles

Code	Profile
AOM	OSI Management
AOM 1	Management Communications
AOM 2	Management Functions
AOM 20	Super Combinations (for further study)
AOM 21	Management Capabilities
AOM 211	General Management Capability (DISP 12060-1)
AOM 212	State and Alarm Management (DISP 12060-2)
AOM 213	Alarm Management (DISP 12060-3)
AOM 22	Event Report Control
AOM 221	General Event Control (DISP 12060-4)
AOM 23	Log Control
AOM 231	General Log Control (DISP 12060-5)
AOM 24	Security (DISP 12060-x)
AOM 241	General Security Capability
AOM 242	Security Alarms
AOM 243	Audit Trail
AOM 244	Access Control
AOM 2441	General Access Control
AOM 2442	Item Rules - Access Control List
AOM 2443	Item Rules - Security Labels
AOM 2444	Item Rules - Capability List
AOM 2445	Global Rules - Access Control List
AOM 2446	Global Rules - Security Labels
AOM 2447	Global Rules - Capability List
AOM 25	Performance
AOM 251	General Performance (pDISP 12060-x)
AOM 252	Metric Objects (pDISP 12060-y)
AOM 2521	Monitor Metric Capability
AOM 25211	General Metric Objects
AOM 2522	Monitor Metric Object
AOM 2523	Mean Monitor Metric Object
AOM 2524	Algorithm Indicating Mean Monitor Metric Object
AOM 2525	Moving Average Mean Monitor Metric Object
AOM 2526	Mean and Variance Monitor Metric Object
AOM 2527	Mean and Percentile Monitor Metric Object
AOM 2528	Mean and Min Max Monitor Metric Object
AOM 253	Summarization Objects (pDISP 12060-z)
AOM 2531	General Summarization Capability
AOM 25311	General Summarization Objects
AOM 2532	Simple Scanner Object
AOM 2533	Dynamic Scanner Object
AOM 2534	Heterogeneous Scanner Object
AOM 2535	Buffered Scanner Object
AOM 2536	Mean Scanner Object
AOM 2537	Mean Variance Scanner Object
AOM 2538	Percentile Scanner Object
AOM 2539	Min Max Scanner Object

Sources: WDTR 10000-2.4, August 1993; [SGFS N 1076], December 1993.

OSI Systems Management has been accepted as a basis for the TMN, which is specifying the use of X.700-series Recommendations. ITU-TS SG VII is thus continuing the maintenance of X.700-series Recommendations, developing additional Recommendations, where needed, to accommodate advances in technology and additional requirements. [Ref. SC21 N 6956 1992]

12.1.5 Military Concerns in Network Management

Some concerns in the OSI management area involve the direction and support of work being done by ISO for Quality of Service (QoS) and multipeer/multiaddressing. Both of these areas were reassessed in 1989 due to lack of support from the nations. Specifically, a formal

question[68] has been raised and put to a ballot on the need for a framework for quality of service within the ISO standards. Since these areas have been found to be priority items for achieving military requirements, it is important for the Nations individually and collectively to express their support for additional work in these standards areas.

The Ad Hoc Working Group on OSI Management (AHWG-OM) of TSGCE SG9 has been formed to address OSI management issues for NATO.[69] The major standing document of the AHWG-OM is *NATO Requirements for Open Systems Management* [Ref. AHWG 1990]; some key elements are the following:

- Part 1: *Rationale and Objective* (of which Section 7 is Military Features and Their Impact on OSI Management and Annex A.2 is the Work Plan), June 1990
- Annex H: *Notes Concerning the Quality of Service Issue,* Third Draft, February 1990
- Appendix 4, *Requirements for a Network Management Broadcast Facility,* May 1990.

12.1.6 Quality of Service (QoS)

In the framework of OSI, QoS provides the capability to measure the service level provided by the communications service provider and the means to request a target service from the communications service provider. QoS parameters now used in ISO standards[70] include transit delay and priority.

SC21/WG1 posed Question 62 (Q62) in 1989 to query whether a QoS Architecture was necessary since such an architecture would require modification to the OSI Reference Model. The first step to developing such an architecture would be defining the components of a QoS Framework. A concern of several national bodies in WG1 is that a new QoS Architecture would destabilize the existing standards. At the May 1990 SC21 Plenary in Seoul, WG1 did not progress the QoS Framework as a new work item. In May 1991, WG1 reported to SC21 the final answer to Q62, saying that there was indeed a need for a QoS framework. [Ref. SC21 N 6158 1991] In June 1991, it was again proposed as a new work item [Ref. SC21 N 6159 1991], which was accepted into the work program in February 1992.

The *Framework on Quality of Service,* August 1993, in development by SC21/WG1 since May 1992, has reached a second working draft [SC21 N 7993] and is expected to become a PDTR at the end of 1994 (initiation of ITU-TS approval expected in 1997). It provides a framework for a coherent treatment of QoS across all OSI standards and extends the current (uncoordinated) QoS requirements. Based largely on X.25, it will support new protocols for multi-media communications in SC6 and time critical communications in TC184, as well as new technologies for public networks. The framework contains the following [Ref. DRA 1994]:

- Common set of concepts and definitions, including a model of the layer and system entities that participate in QoS
- Collection of definitions of QoS mechanisms, such as negotiation procedures.

---

68 ISO/IEC JTC1/SC21/WG1 Question 62: "Is Quality of Service an architectural issue which needs overall guidance and consistent approach across all layers?" Balloting closed in May 1989.

69 The work TSGCE SG9 working groups is discussed in Section 17.3. The AHWG-OM is addressed in Section 17.3.5.

70 ISO/IEC references to QoS are in Layer 3 (ISO 8438), Layer 4 (ISO 8072, 8073), Layer 5 (ISO 8326), Layer 6 (ISO 8822), and Layer 7 (ISO 8649, 8650, 8571-3).

Issues not yet resolved in the August 1993 QoS Framework are treatment of guaranteed QoS, sharing of systems management information, use of QoS by applications, dynamic use of QoS, and predictability and confidence levels including issues of precision and granularity [Ref. SC21 N 7992]. A separate document [SC6 N 7989] of SC6 identifies and categorizes QoS parameters [Ref. SC21 N 8262 1993].

In the 1993-1996 Study Period, ITU-TS SG7 will continue to study the question of Network Performance and Quality of Service in Data Communication Networks (Study Question 4). [Ref. SC21 N 6956 1992] In October 1993, SG7 informed SC21 that SG7 had agreed to collaborate with SC21 to develop the architecture for OSI QoS, covering all seven of the OSI layers, with the stated intention to make the result an ITU-TS recommendation [Ref. SC21 N 8263 1993].

The AHWG-OM has identified [Ref. SG9/WG1 1990a; AHWG-OM 1989] the following deficiencies and requirements relative to QoS:

- Only static QoS parameters have been defined—the relationship of various QoS parameters to each other and actions to take upon dynamic change in QoS are not yet supported.
- A tight coupling between QoS and communications services is needed to support applications in areas such as military and real-time process control and high assurance of message delivery. Specifically, this means that applications need:
    - Capability to clearly express the QoS requirement to the underlying communications service
    - Notification of changes in QoS
    - Close monitoring of the QoS
    - Assurance that QoS is maintained in a deterministic manner.
- While QoS's need of the layer services have led to protocol definitions that include parameters for specifying QoS, no syntax or semantic meaning of those parameters has been defined.

Further, the AHWG-OM has recommended that:

- An overall framework for OSI QoS be developed and, specifically, ISO/IEC SC21/WG1 raise the priority of QoS discussions in this area.
- QoS be expanded to provide five functions: establishment, monitoring, maintenance, notification of change, and negotiation.
- The definition of QoS be modified to include the following four classes of QoS parameters:
    - Quality of addressing—the correct assignment of addresses to the originator and the recipient.
    - Quality of message—the reliability of message delivery against data loss, data corruption or insertion, misdelivery, duplicate delivery, or out-of-sequence delivery.
    - Quality of timeliness—the delay of transferring information across a communications service, including specification of requirements on time limits for delivery of a message. The latter may be in terms of the time after which the message is no longer valid, allowable delay in the transfer, and the action to take on failure to meet the criteria.
    - Quality of confidentiality—the ability of the system to protect its resources from unauthorized use and to prevent unauthorized interception of information relative to the transfer of a message. Clearly this quality overlaps security requirements.

The AHWG-OM in its meeting in June 1990 recommended three steps for progressing work on QoS: (1) establish an ad hoc working group on QoS in TSGCE SG9 to define QoS requirements and a QoS Framework; (2) apply the QoS Framework in other SG9 working groups; and (3) provide additional information to ISO and other standards bodies on the need for QoS. AHWG-OM recommended that the proposed framework consider the application QoS parameters, the application actions (procedures used by applications in processing QoS information), and QoS facilities for establishment, monitoring, maintenance, notification, and negotiation of QoS. [Ref. AHWG 1990a]

A key background paper for QoS is *Management Requirements Arising from a NATO Study of Quality of Service*. [Ref. Kennedy 1989] This paper identifies QoS requirements in such areas as specification, establishment, application actions, monitoring, maintenance, notification, negotiation, information flow, and applicability. It also addresses the QoS framework, information model, and interaction model. Four QoS parameters are identified: addressing, message, timeliness, and confidentiality. The June 1990 recommendations of the AHWG-OM to SG9 were based, in part, on material described in this paper.

12.1.7 Special Interest Groups for OSI Management

A number of special interest groups have been formed to promote standardization of OSI management. These include [Ref. AHWG 1990b]:

- Network Management Experts Group—formed within EWOS with plans to meet four times per year.
- Network Management Forum (NMForum)—developing a roadmap (EWOS/TZ/91/214), an industry-accepted, standards-based concept that promotes product interoperability. The Roadmap plan is a path consisting of a series of points in time (OMNIPoints). At each point it is agreed that it is sensible to build interoperable management products to agreed interfaces with agreed functionality. [Ref. OSN 1992e] The first OMNIPoint was published in October 1992 and brings together SNMP (see Section 12.1.9) and CMIP (X.700) standards. It is already referenced in the US Government Network Management Profile (GNMP). [Ref. OSN 1992f]
- NIST Network Management Special Interest Group (NMSIG)—developing specifications for the *Stable Implementor's Workshop Agreements* with a target date of December 1990. The 1990 version will define, in coordination with EWOS and the NMForum, managed objects for LANs including FDDI, X.25, and ISDN. Additional managed objects would be defined in 1991 for Layer 3-7 protocols and routers and in 1992 for applications, operating systems, and database management systems.

12.1.8 ECMA Model for Management

In January 1987 the European Computer Manufacturers Association (ECMA) established [Ref. ECMA 1987] an abstract model for the management aspects of OSI. The framework provided by ECMA is designed to form the basis for the definition and specification of services and protocols that enable the planning, organizing, supervising, and controlling of the communication service that forms a part of a distributed information processing system. In this context, OSI management is defined as the collection and interchange of information necessary for the management of those aspects of open systems that are relevant to Open Systems Interconnection. The abstract model addresses standardization in two areas:

- Semantics of the management information transferred or extracted from the management information base (where the structure of the information within the

management information base is viewed as a local matter and not subject to management standardization)

- Services and associated protocols for the transfer of management information between open systems; this requires that both the syntax and semantics of the information transferred be specified.

ISO standards for OSI network management are being developed by SC21/WG4; they are discussed in Section 12.1.3.

12.1.9 Simple Network Management Protocol (SNMP)

While OSI Systems Management, CMIP is designed for use in an OSI environment, SNMP is designed to operate over TCP/IP (see Section 9.7.4). A new version of SNMP (SNMPv2) has been issued as a draft standard. It addresses many of the deficiencies present in the original SNMP and is intended for use in both TCP/IP and OSI environments. While OSI Systems Management provides a more powerful and flexible scheme for representing management information and offers a richer set of structuring tools, SNMPv2 may enjoy an advantage in Security. SNMPv2 includes a well-defined, easily-understood security facility consisting of access control, authentication, and privacy. [Ref. Stallings 1993]

12.1.10 Desktop Management Interface (DMI)

The Desktop Management Interface (DMI) standard (see Section 15.1.3.10) aims to standardize how desktop systems make status and configuration information available to network management applications. Vendors committed to supporting this standard include Novell, Digital, IBM, Intel, Microsoft, Sun-Connect, and SynOptics. A key part of DMI is the Management Information File (MIF), a database of status and configuration information generated by components (e.g., peripherals, personal computers) in the network. DMI-compliant management applications running on a system such as HP's OpenView can collect the information from the desktop to do inventory management, accounting, and real-time diagnostics. [Ref. RNLA 1994, pp. 29-30]

12.2 Standards for Conformance Testing

Conformance testing is crucial to the achievement of OSI to ensure comparability of test procedures and results by different test centers. Conformance testing is defined by the United Kingdom's National Centre for Information Technology as [Ref. Pink 1991] as "the testing of a product against a published standard in order to determine the degree of conformance with that standard."

12.2.1 Conformance Testing Methodology, Framework, Issues, and Assessment

12.2.1.1 ISO/IEC 9646 on Conformance Testing Methodology and Framework

Standardization of conformance test suites needs to be based on a standard testing methodology and approach to test suite specification, which is reflected in ISO/IEC 9646, *OSI Conformance Testing Methodology and Framework (CTMF)*. Work has already begun in standardizing test suites based on ISO/IEC 9646 for X.25 terminals, the connection-oriented transport protocol (ISO 8073), MHS, FTAM, ACSEs, session, and presentation protocols. A

detailed description of OSI conformance testing is provided in [Ref. Rayner 1987]. ISO/IEC work in conformance testing is done by SC21/WG1.

ISO/IEC 9646 is being developed in seven parts, five of which have achieved IS status. The seven parts, together with the current amendments, are as follows [Ref. DRA 1994]:

- ISO/IEC 9646-1 (Part 1): *General Model*, July 1991 (ITU-TS X.290)—gives an overview of the conformance testing process by introducing the basic ideas of the meaning of conformance, implementation conformance statements, test methods, test suites and their components, and general terminology. A revision incorporating the following two amendments is in progress (IS text expected March 1994):
  - AM 1, *Protocol Profile and Multi-Protocol Testing*, October 1993 [SC21 N 7321]
  - AM 2, *Multi-Party Testing*, October 1993 [SC21 N 7322]
- ISO/IEC 9646-2 (Part 2): *Abstract Test Suite Specification*, July 1991 (ITU-TS X.291)—applies to test suite suppliers, defines in detail the different test methods, and gives requirements and guidance for the test suite development process applicable to base protocol standards. A revision incorporating the following two amendments is in progress (IS text expected March 1994):
  - AM 1, *Protocol Profile and Multi-Protocol Testing*, October 1993 [SC21 N 7323]
  - AM 2, *Multi-Party Testing*, October 1993 [SC21 N 7324]
- ISO/IEC 9646-3 (Part 3): *The Tree and Tabular Combined Notation (TTCN)*, October 1991 (ITU-TS X.292)—defines he test specification language recommended for standardized test suites in all the layers of the OSI Reference Model except the Physical Layer. It enables abstract test suites to be written in sufficient detail to determine unambiguously the verdicts to be assigned when test cases are run without being specific to a given executable language or test system. It has both a human readable (TTCN.GR) and a machine-processable (TTCN.MP) form.
  - AM 1, *TTCN Extensions*, October 1993 [SC21 N 7528]
  - DAM 2, *TTCN Further Extensions*, December 1993 [SC21 N 8374]
- ISO/IEC 9646-4 (Part 4): *Test Realization*, May 1991 (ITU-TS X.293)—applies to test realizers and gives requirements and guidance for the production of a means of testing an abstract test suite. The means of testing encompasses the test system, the executable test suite, the means of performing test selection and parameterization, and the means of realizing control and observation of the system under test. The main requirements concern the means of production of a conformance log to present what occurred during testing in a way that is human-readable and related to the abstract test cases concerned. A revision incorporating the following two amendments is in progress (IS text expected March 1994):
  - AM 1, *Protocol Profile and Multi-Protocol Testing*, October 1993 [SC21 N 7325]
  - AM 2, *Multi-Party Testing*, October 1993 [SC21 N 7326]
- ISO/IEC 9646-5 (Part 5): *Requirements on Test Laboratories and Clients for the Conformance Assessment Process*, May 1991 (ITU-TS X.294)—specifies requirements and gives additional guidance for both the test laboratory and the client for the whole of the conformance assessment process (i.e., before, during, and after the execution of the selected test cases). General proformas are provided for test reports. Accreditation bodies look for compliance of test laboratories to this part when they assess OSI test laboratories for accreditation. A revision incorporating the following two amendments is in progress (IS text expected March 1994):
  - AM 1, *Protocol Profile and Multi-Protocol Testing*, October 1993 [SC21 N 7327]
  - AM 2, *Multi-Party Testing*, October 1993 [SC21 N 7328]

- ISO/IEC 9646-6 (Part 6): *Protocol Profile Testing Specification,* October 1993 [SC21 N 7329] (balloting ended April 1993 and editing meeting held September 1993)—equivalent to Part 2 for profiles rather than for individual protocols; give guidance on the meaning of conformance to a profile and gives requirements and guidance for the profile test specification process.
- DIS 9646-7 (Part 7): *Requirements and Guidelines on Implementation Conformance Statement (ICS) and ICS Proformas,* October 1993 [SC21 N 8180] (balloting ends April 1994)—specifies requirements and guidance on statements made to claim conformance for a product to one or more OSI specifications. It draws together and generalizes information on this subject from a variety of older sources, including Parts 2 and 6 of ISO/IEC 9646 and ISO/IEC TR 10000-1. It applies to statements made for conformance to protocols, protocol profiles, and information objects. When such an implementation conformance statement is used in conformance testing, it determines which options are to be tested.

The amendments noted above have the following scope:

- *Protocol Profile Conformance Testing Methodology* (PPTM) extends the OSI conformance testing methodology and framework (ISO/IEC 9646) to make it applicable to OSI protocol profiles as well as base protocols. This standard supersedes TR 10000-1 as far as conformance aspects are concerned.
- *Multi-party Test Methods (MPTM)* addenda define the main requirements concerning MPTM and a multi-party test architectural model. The model will be used to map abstract test methods on which to base the development of abstract test suites and means of testing for the various multi-party protocols and multi-party testing configurations using more than one protocol or more than one channel.
- *TTCN Extensions* introduces the notion of parallelism in order to ease the writing of test cases, provide a language means to describe explicitly the cooperation of (distributed) components of a test architecture, and to make TTCN a test notation that covers the aspects of a multi-party test methodology.

Additional topics to be addressed for conformance testing are ISDN and multimedia concerns, application of formal methods; and protocols for test support.

12.2.1.2 Other Conformance Testing Standards Work

Formal Methods. *Formal Methods in Conformance Testing (FMCT)* is a complementary standard to ISO/IEC 9646 that specifies a general methodology for performing conformance of a protocol implementation, given a formal specification of the protocol standard. It includes the following [Ref. DRA 1994]:

- Establishment of a theory and framework leading to a formal testing methodology that may be used to establish and assess conformance of an implementation under test (IUT) to behaviors described in the formal description of the protocol
- Definition of a test methodology that includes descriptions of test entities (e.g., upper/lower testers, protocol entities augmented with testing functions) applicable to single-layer, multi-layer, and multi-party conformance testing
- Definition of a methodology for automatic generation and validation of test suites from formally specified protocol entities.

It is currently in WD status [SC21 N 7995, September 1993] with a collaborative meeting with ITU-TS SG10(Q/10) in February-March 1994; CD text is expected in June 1994 and initiation of the ITU-TS ballot approval in 1997.

SC21/WG9. A joint working group (WG9) was established by SC21 in June 1993 to publish a technical report on the topic: interpretation of accreditation requirements as specified in ISO Guide 25 for information technology and telecommunications testing laboratories for software and communications testing services. Publication is expected December 1994.

Testing with Non-OSI Protocols. Two new work items related to non-OSI protocols were approved by the SC21 Plenary in June 1993 to be forwarded to SC21:

- *Conformance Testing of OSI Protocols over OSI Services Provided by Non-OSI Protocols* [SC21 N 8011, July 1993]
- *Extensions to ISO/IEC 9646 on Testing of OSI Protocols over OSI Services Provided by Non-OSI Protocols* [SC21 N 8016, June 1993]

These would address some of the testing issues associated with coexisting protocol stacks from the Internet (TCP/IP) and OSI. The first proposal [SC21 N 8011, August 1993] was not accepted by JTC1.

Conformity Assessment. At its March 1993 Plenary in Berlin, JTC1 established a standing Special Working Group on Conformity Assessment (SWG-CA). The first meeting was held in September 1993 and another in January 1994. [Ref. SC21 N 7713 1993] SC21 approved a new work item proposal to be forwarded to JTC1 on *Open Systems Assessment Methodology* [SC21 N 8010, June 1993]; this proposal would have generalized ISO/IEC 9646 to Open Distributed Processing (ODP), open system environment (OSE) profiles, and network management standards, but it was not accepted by JTC1.

Work on ODP conformance testing was the basis of the new work item on Open Systems Assessment. Clearly, much of the OSI conformance testing methodology and framework can be applied to ODP, and, some extent, this has already been done in specifications of the Protocol Profile Testing Methodology, Multi-Party Testing Methodology, and Implementation Conformance Statements. The proposed new work item would have addressed the necessary terminology and general concepts applicable to OSE profiles, APIs, and network management, as well as to ODP. [Ref. SC21 N 8010 1993]

Convergence of conformance testing methodologies for OSI and ODP will need to be addressed, whether or not the conformity assessment methodology is finally accepted in some revised (reduced scope) form. In December 1993, the JTC1/SGFS requested SC21/WG1 and SC22/WG15 to investigate convergence of their activity on conformance testing and development of a plan and time table for convergence if practical, or a rationale for concluding convergence is not practical. In the latter case, the SGFS asked for recommendations on how to proceed with overlapping OSE and ODP requirements in this area. (Conformity assessment related to OSE is addressed in Section 15.3).

Testing Secure Open Systems. The UK National Physical Laboratory has prepared a report, *The Requirement for a Methodology to Test Secure Open Systems,* September 1993. This report outlines the required framework for a methodology that integrates conformance testing and security evaluation, as a means to test secure open systems.

12.2.1.3 Conformance Testing Issues

SC21/WG1 has noted concerns [Ref. SC21 N 4187 1989] about the available resources and direction of work on upper layer conformance testing. Work has slipped 2 years on abstract test suites for FTAM and 3 years for embedded test suites for ACSE, Presentation Layer, and

Session Layer. There is an imbalance between work on the basic methodology and that applied to the actual conformance tests, specifically on abstract test suites.

Moreover, some OSI certification agencies will not certify FTAM implementations as conformant when the implementation, in the role of an initiator, does not employ all possible protocol variations, even though the protocols that are used completely support the services of that implementation. Although the problem presently concerns FTAM, the same problems will occur in products implementing other standards where there is an asymmetric relationship between correspondents and where the initiator controls the protocol that will be exchanged. The United States therefore recommends that SC21 begin the following efforts [Ref. X3 1992e]:

- ISO/IEC 9646 be amended to give warning and guidance for standards needing to incorporate a clause describing the conformance requirements for the sender aspects of the protocol.
- Those standards with specific sender requirements must clarify their claims of conformance to indicate permitted conformance subsets.
- Upcoming standardized APIs will mandate the need for service testing. SC21 should begin studying the relationships between protocol machines and the service/user interface.
- SC21 should reaffirm that conformance statements about the definition of conformance subsets are the responsibility of base standards, not of Registration Authority Test Labs, workshops, etc.
- It should be possible to allow PICS to describe varied protocol uses based on the context in which the protocol machine is used.

Other conformance-related problems have been noted. The concepts of general and dependent conformance are being misused and misunderstood (see also Section 12.1.2.5). An ISO/IEC-ITU-TS Joint OSI Conformance Group Interim Meeting in Durham, North Carolina, in November 1991 issued a health warning on this topic for general consumption and produced a liaison statement to WG4 in the hope that some National Bodies would take note of the concerns in relation to any relevant ballots. Furthermore, there are serious problems with the double column status notation meaning and use. Again, a health warning paper was produced. [Ref. SC21 N 6819 1992]

Since there is as yet no suitable home for information relating OSI conformance to ODP conformance, a new question was to be raised at the Plenary in June 1992 to tackle this problem. Finally, there were inadequate contributions to progress any of the further TTCN extension topics satisfactorily. Therefore, DAM 2 to 9646-3 includes calls for contributions on all other topics. [Ref. SC21 N 6819 1992]

In May 1992, the UK proposed a new question (Q1/69) on conformance assessment for OSI security in order to assess the proper scope for a new work item proposal and the appropriate time scale for it. A basic assumption of the ISO/IEC 9646 conformance testing methodology is that bugs in an implementation will be unintentional and therefore not deliberately hidden. In OSI security this assumption is false, and there is a need to test implementations for breaches of security such as Trojan horses, trap doors, or viruses. [Ref. SC21 N 7098 1992]

EWOS has agreed [ITSTC 1989] to convene an activity to study and investigate OSI Conformance Testing Methodology. This work would examine central aspects of OSI testing methodology that are necessary to support standardization of test specifications. CEN has been assigned leadership of the work.

12.2.1.4 TTCN

TTCN (ISO/IEC 9646-3) is a unique, informal notation that was developed by ISO and ITU-TS for specifying generic and abstract test cases. Other formal description techniques in use for this purpose are the Language of Temporal Ordering of Specification (LOTOS) and Estelle—both accepted in the *NTIS Transition Strategy*—and the System Development Language (SDL), developed by ITU-TS (Recommendation Z.100). Both Estelle and SDL are Pascal-based notations. These formal description techniques (FDTs) are described in detail in Section 12.2.3.

TTCN provides a notation in which generic and abstract test cases can be expressed in test suite standards; which is independent of test methods, layers, and protocols; and which reflects the abstract testing methodology of ISO/IEC 9646. TTCN provides a naming structure to reflect the position of test cases in the abstract test suite hierarchy (complete test suite, test groups, test cases, test steps, and test events). TTCN also provides the means of structuring test cases as a hierarchy of test steps culminating in test events.

EWOS has circulated for ratification a revision of *The TTCN Style Guide,* EWOS Technical Guide 025 (Revision 1), October 1993. ETSI intends to use the document on a field trial basis before formally approving it.

12.2.1.5 Organizations Contributing to Conformance Testing

Many organizations other than ISO/IEC have been formed to address OSI conformance testing. These include Corporation for Open System (COS), OSINET, Standards Action and Promotion Group (SPAG, European Committee for Standardization (CEN)/European Committee for Electrotechnical Standardization (CENELEC), NIST, Industrial Technology Institute (ITI), World Federation of Manufacturing Automation Protocol (MAP) and Technical and Office Protocol (TOP) User Groups, Conformance Testing Services-Wide Area Network (CTS-WAN), National Computing Centre (NCC), and EurOSInet. TSGCE SG9 is addressing [Ref. CA 1989] military requirements in this area and whether NATO-specific activities need to be supported. The following are areas in which existing civil organizations may be expected to contribute to conformance testing to support military requirements [Ref. Cardonna 1988]:

- Developing standards and conformance certification criteria: ISO, ITU-TS
- Developing abstract test suites for OSI upper layers: ISO
- Developing test profiles and provisioning testing under military requirements: COS, SPAG
- Developing site accreditation criteria: Industrial Technology Institute (ITI)
- Implementing site accreditation and testing tools, and specifying test control and maintenance procedures: NIST
- Developing standards and test methodologies: CEN/CENELEC, ANSI.

COS [Ref. COS 1989] and SPAG have now completed formal agreement to combine their conformance test products within a single integrated tool set (ITS). In addition, COS, POSI, and SPAG have completed (June 1989) an Initial Strategic Technical Cooperation Agreement that commits the organizations to a strategic cooperative arrangement designed to provide a common technical solution to conformance testing, building upon the ITS. The agreement is also known as "CPS" (both for Conformance Promotion Strategy and for COS-POSI-SPAG).

OSINET, a 55-member United States-based interoperability testing organization, has voted to reorganize under the auspices of COS. OSINET was formed in 1984 under the auspices of NIST to work in three specific areas:

- Research and development of test scripts used in OSI interoperability testing
- Interoperability testing and registration of announced OSI products
- Demonstration and promotion of OSI technology [Ref. OSN 1991h].

There is a need to harmonize testing and certification schemes to enable mutual recognition of results of testing internationally. In 1985, the Conformance Test Service (CTS) was set up under the CEN/CENELEC to support the development of test tools and provision of test services. In Phase I (1985-1986), it addressed the following topics: OSI protocols, software quality, programming languages, and GKS. In Phase II (1987-1988), it continued to address OSI protocols as well as SGML, ODA, POSIX, and the programming language C. Memorandum M-IT-03 defines a framework for testing and certification in Europe which aims to enable mutual recognition of results of testing. The European Committee for IT Testing and Certification (ECITC) is implementing M-IT-03 by setting up mechanisms for mutual recognition of test reports and certificates These include abstract test suites and recognition of test tools, services, and tested products. The Open Systems Testing Consortium (OSTC) was formed in 1989 on completion of the CTS project to ensure continued harmonization. [Ref. Pink 1991]

12.2.2 PICS Proformas

An approach used in conformance testing (and in other applications) to specify interoperability parameters for an implementation profile (or a functional profile) is called a protocol implementation conformance statement (PICS). A PICS specifies all the parameters and options required to show how a particular implementation meets static conformance requirements. As such, it is the first tool in conformance testing. A PICS proforma is a PICS template developed and standardized in conjunction with a protocol standard. In the future, a PICS proforma can be expected to be required as part of the functional profile guidelines being developed by NIST, EWOS, AOW, NATO, and other standards bodies.

There are many projects involving the development of PICS proformas, including an Annex of ISO/IEC 9646-2, *Guidelines for PICS Proformas*, *Guidelines for PICS Proformas in SC6*, *Catalogue of PICS Proforma Notations*, and TR 10000-1. The Arles meeting of SC21 in May 1991 initiated an NP for ISO/IEC 9646-7 to put in one place all of the agreed requirements and guidance related to PICS, Profile Implementation Conformance Statements (ICSs), and Information Object ICSs.

Confusion has recently arisen regarding the use of the PICS in the conformance assessment process. Specifically, does the PICS describe the supplier's product or the supplier's protocol implementation? The United States contends that it is the latter and proposes that clarifying text be added to ISO 9646-7. [Ref. SC21 WG1 N 1156 1992]

12.2.3 Formal Description Techniques (FDTs)

FDTs are used to produce unambiguous descriptions of OSI services and protocols in a more precise and comprehensive way than natural language descriptions. Further, FDTs provide a foundation for analysis and verification of a description. The objectives of FDTs are to provide [Ref. DRA 1994]:

- Unambiguous, clear, and concise specifications
- Basis for determining completeness of specifications
- Foundation for analyzing specifications for correctness, efficiency, etc.
- Basis for determining consistency of specifications relative to each other
- Basis for implementation support.

There are three international standard FDTs that range from abstract to implementation-oriented: Estelle, LOTOS, and SDL. Since emerging standards are being written in one or more of these FDTs, subsections are provided below to give some technical information together with the basis, derivation, and character, for these description techniques. TR 10167, *Guidelines for the Application of Estelle, LOTOS, and SDL*, July 1991, provides guidelines for applying these three FDTs. A fourth FDT—TTCN (ISO/IEC 9646-3)—was described in Section 12.2.1.4 above.

SC21/WG1 developed a working draft for *Architectural Semantics for FDTs* [SC21 N 4231, April 1990]. This work was planned to assist development of formal descriptions of standards for data communications, networking, and distributed computing. The draft defines and catalogues a set of selected elementary concepts, which act as a bridge between the architectural concepts and structures and the semantic models of the FDTs (Estelle, LOTOS, and SDL). SC21 approved the May 1990 recommendations developed by a reassessment of the work associated with the *Architectural Semantics for FDTs*. The current work in SC21/WG1 will be terminated and a subproject initiated in SC21/WG7 in the area of ODP architectural semantics. [Ref. SC21 N 4655 1990]

An article by L. Simon and L.S. Marshall entitled, "Using VDM to Specify OSI Managed Objects," in *Proceedings of Third International Conference on Formal Description Techniques (FORTE '91)*, November 1991, Sydney, is an example of the use of FDTs in the definition of the behavior of managed objects. [Ref. SC21 N 7140 1992]

12.2.3.1 Estelle

Estelle (ISO 9074, *Estelle, A Formal Description Technique Based on an Extended State Transition Model*, July 1989) is a formally-defined specification language for describing distributed or concurrent processing systems, in particular those that implement OSI services and protocols. The language is based on widely used and accepted concepts of communicating non-deterministic state machines (automata). An Estelle specification defines a system of hierarchically-structured state machines. The machines communicate by exchanging messages through bidirectional channels connecting their communications ports. These messages are queued at either end of the channel. The actions of machines are specified in (extended) Pascal; hence, familiarity with Pascal makes Estelle specifications easily readable. Estelle uses Pascal data types in its data descriptions.

Estelle is based on an extended state transition model, i.e., a model of a nondeterministic communicating automaton extended by the addition of the Pascal language. Estelle may be viewed as a set of extensions to Level 0 of ISO 7185 (*Programming Language - Pascal*) that models a specified system as a hierarchical structure of communicating automata that may run in parallel and may communicate by exchanging messages and by sharing, in a restricted way, some variables. As in Pascal, all manipulated objects are strongly typed, which enables static detection (e.g., during compilation) of specification inconsistencies.

Estelle language mechanisms allow modelling of synchronous and asynchronous parallelism between state machines of a specified system. They also permit dynamic development of the system configuration. Estelle specifications can be prepared at different levels of abstraction, from abstract to quite implementation-oriented. The latter may be derived from the former with the aid of supporting tools. An Estelle tutorial has been developed (ISO 9074 AM 1, January 1992). ISO 9074, Estelle, is undergoing revision to include Amendment 1. This second edition is scheduled to reach IS status in December 1994.

12.2.3.2 LOTOS

LOTOS (ISO 8807, *LOTOS, A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour,* February 1989) is a mathematically-defined FDT, developed from a large, well-established body of theory based on three mathematical techniques: Calculus of Communicating Systems (CCS), Communicating Sequential Processes (CSP), and ACT ONE. Having a well-defined mathematical foundation, it provides a solid basis for both analysis and development of reliable tools, including simulation, compilation, and test sequence derivation. The basic constructs of LOTOS allow modelling of sequencing, choice, concurrency, and nondeterminism in an entirely unambiguous way. In addition, LOTOS permits modelling of both synchronous and asynchronous communication. LOTOS, like SDL, uses abstract data types in its data descriptions.

LOTOS may be applied to produce a specification of the allowed behaviors of a system, i.e., the set of all behaviors that may be observed of a conforming implementation. Furthermore, LOTOS permits the description of allowed behaviors without describing how this may be achieved or by describing particular mechanisms that achieve the required behavior.

Formal descriptions of the session service and protocol using LOTOS have been developed:

- TR 9571, *LOTOS Description of the Session Service,* September 1989
- TR 9572, *LOTOS Description of the Session Protocol,* September 1989.

WG6 has developed PDTRs for a *LOTOS Description of the CCR Service,* PDTR 11589 [SC21 N 7876, June 1993] and *Protocol* PDTR 11590 [SC21 N 7877, June 1993] (see Section 9.11.3.2).

In addition, WG1 proposed a new sub-question on LOTOS enhancements to redress limitations identified by experience to date with the language. The sub-question received strong support in balloting, and it has been proposed that a NWI on LOTOS enhancements be initiated. The following is a list of possible enhancements in priority order [Ref. SC21 N 7096 1992]:

- Define a more user-friendly notation for data-type descriptions
- Compose a specification from pre-existing modules to promote reusability and structuring
- Consider mechanisms to remove the inability to express partial synchronization and data exchange
- Consider enhancements to allow specifying time and priorities.

An NP on Enhancements to LOTOS [SC21 N 8022] has gone out to SC21 for letter ballot on whether or not NBs can commit to actively participate in its development. The current draft of this standard is *Initial Draft on Enhancements to LOTOS,* November 1993 [SC21 N 8023].

The European Strategic Programme of Research and Development in Information Technology (ESPRIT) LOTOSPHERE Project conducted a study from November 1990 to April 1992 on language enhancements to LOTOS, which resulted in a deliverable on language enhancements. While the proposal has not been elaborated to the point that text can be used directly for the revision of LOTOS ISO 8807, it is believed to form an excellent basis for the production of such a revision. [Ref. SC21 WG1 N 1157 1992]

12.2.3.3 SDL

SDL is based (ITU-TS Z.100-Series recommendations) on the extended finite state machine model supplemented by capabilities for abstract data types based on the initial algebra model (the same one used in the ACT ONE part of LOTOS). This combination is supported by well-defined formal semantics. SDL provides constructs to present structures, behaviors, interfaces, and communications links. In addition, it provides constructs for abstraction, module encapsulation, and refinement. All of these constructs were designed to assist the representation of a variety of telecommunications systems specifications, including aspects of protocols and services.

12.2.3.4 G-LOTOS

A standard for a graphical syntax, G-LOTOS, has recently been approved that provides an extension to LOTOS (ISO 8807/AM 1) to facilitate production and enhance clarity and readability of formal descriptions, simplify teaching and learning the language, favor the development of advanced user-friendly software tools, and promote the diffusion and application of the language.

12.2.3.5 Z Specification Language

Z is an abstract specification language; however, there is no current standard for Z. Z is based on the mathematics of set theory and predicate calculus. Systems are described by introducing fixed sets and variables and specifying the relationship between them. Current applications of Z include safety- and security-critical systems. [Ref. Spivey 1989] ISO/ITU-TS Joint Modelling Group has suggested Z be considered as a candidate FDT for use in ODP [Ref. SC21 N 6088 1991].

12.2.4 Conformance Test Suites

Before conformance testing can be conducted, conformance test suites must be specified for each standard to be addressed. The standards for conformance test suites typically have two parts: *Test Suite Structure and Test Purposes* and *Abstract Test Suite*.[71] These form the basis for developing a conformance test and verifying its accuracy. Examples of standards for conformance testing are DIS 8825-4 (Presentation Protocol) ISO 8882-2 (X.25), ISO/IEC 10025-2 (COTP over CONS), DIS 10168 (Session Protocol), ISO/IEC 10169 (ACSE Protocol), ISO/IEC 10170 (FTAM), ISO/IEC 10729 (Presentation Protocol), and ISO/IEC 10739-1 (Virtual Terminal).

In 1989, NIST conducted an analysis of the OSI testing situation and concluded that unless it acted, no credible means of substantiating GOSIP compliance would be available in time to support the US Government OSI mandate beginning August 1990. Abstract Test Suites, where they existed, were fragmented and not publicly available. Although multiple suppliers of Means of

[71] A third kind, Generic Test Suites, are no longer recognized by ISO 9646.

Testing (MOTs) existed, no credible mechanism existed to assess MOTs against GOSIP requirements; no means existed for finding one MOT acceptable and another not. Moreover, no program of evaluating and accrediting commercial GOSIP testing laboratories was planned. From April through November 1989, NIST defined a GOSIP Testing Program and on November 13 issued a proposed *GOSIP Conformance and Interoperation Testing and Registration* FIPS for public comment. [Ref. Favreau 1990] On September 1990, NIST published the initial set of registers (*Register of Abstract Test Suites* and *Register of Assessed Means of Testing* (MOTs)). The *Register of Accredited Testing Laboratories* appeared May 1991 [Ref. Martin 1991] and now contains more than 30 MOTs for GOSIP Version 1.0 protocols. The US GOSIP Register Database (GRD) is an on-line database facility developed by NIST that provides up-to-date reference information on the seven GOSIP registers that are currently available. It can be accessed via the Internet or directly via a modem. [Ref. Favreau 1992] Section 10.2.1.2 addresses the POSIX Conformance Test Suite.

12.3 Standards for Registration Authorities

Registration provides unambiguous identification of instances of certain types of information objects within the OSI environment. Examples of these instances are an application process, an application entity, and the definition of a class of information such as a file format. Registration is the assignment of an unambiguous name to an instance of a type of information object in a way that makes the assignment available to interested parties. It is carried out by a registration agent that may be either a standard or an organization.

SC21 and ITU-TS SGVII have agreed to collaborate in work on registration authorities. The groups have concurred that "the establishment and operation of registration is critical to communications in a distributed environment and that, without procedures for the operation of registration, interoperability between applications is unlikely". [Ref. SC21 N 5014 1990] An area of disagreement is the presence of the Name Form in ISO 9834-1, included to support the specification of procedures to ensure the assignment of unambiguous names for registration purposes.

SC21/WG1 has developed[72] a standard (ISO/IEC 9834, *Procedures for the Operation of OSI Registration Authorities*) for the operation of OSI registration authorities. The status and structure of this standard is as follows:

- ISO 9834-1 (Part 1): *General Procedures*, April 1993 (ITU-TS X.660).
  - PDAM 1, *Object Identifier Component for Short Form Names*
  - WDAM 2, *Incorporate Definition of Root Arcs of Object Identifier Tree* (WDAM expected August 1994, PDAM December 1994, DAM December 1995, and AM December 1996)
- ISO 9834-2 (Part 2): *Registration Procedures for Document Types*, November 1993 [SC21 N 8149] (ITU-TS X.661:1992); document types are defined in ISO/IEC ISP 10607.
- ISO 9834-3 (Part 3): *Registration of Object Identifier Component Values for Joint ISO/ITU-TS Use*, July 1990 (ITU-TS X.662:1992). An amendment is being prepared to align this part with Part 1; PDAM expected December 1994. A further amendment dealing with RH-name-tree has been recommended by ITU-TS [SC21 N 7577]. An internal SC21 document, last updated in August 1991 [SC21 N 6370], is

72 Work on Registration Authorities beginning in November 1989 was transferred to SC21/WG6.

maintained for register of object identifier components allocated to areas of joint ISO-ITU-TS work.

- ISO 9834-4 (Part 4): *Registration of VTE Profiles,* December 1991 (ITU-TS X.663:1992).
- ISO 9834-5 (Part 5): *Registration of VT Control Objects,* December 1991 (ITU-TS X.664:1992).
- ISO 9834-6 (Part 6): *Registration of AP Titles and AE Titles,* November 1993 (ITU-TS X.665:1992).

Work on registration authorities (SC21/WG1) is ongoing in one additional area—registration of system titles, but this will probably be incorporated in the management standards. Prior work on authentication mechanisms, application context names, abstract syntaxes, and transfer syntaxes (WD 9834-7, 8, 9, B and C) is now considered as not required.

Question Q1/49.8 concerning conformance and registration asks "What are the conformance implications of the registration of an item for a system that supports the use of that item in conjunction with relevant OSI protocols to which it is claimed to conform?" The answer, which was approved in November 1992 [Ref. SC21 N 7471 1992], states that those requirements which are clearly requirements to be met by implementations are conformance requirements and should be testable in accordance with ISO/IEC 9646. However, those requirements that are not to be met wholly or partially by users of OSI systems are not testable, not conformance requirements, and not compliance requirements. They are called usage requirements.

ITU-TS Q23/VII, in a liaison statement to SC21, suggested that SC21 initiate a joint work to amend ISO 9834-3 to pertain to the join arc in the RH-name-tree, rather than the SCN.1 tree. [Ref. SC21 N 7577 1993]

12.4 Assessment

Quality of Service and security are not well addressed by OSI and other open systems standards. Both of these sets of services require review and possible modification of the basic reference models for open systems. They therefore could lead to disruption of some of the standards that have already become stable under the existing reference models.

Both sets of services may be supported in a wide range of ways, and several approaches of these may be required in information systems to meet operational requirements. For example, quality of service affects all the layers of the OSI Reference Model, and the associated protocols, managed objects, and parameters of the protocol data units may all have to be extended to meet military requirements. Security can be expected to impact at least the Physical, Network, and Applications Layers of the OSI Reference Model (the NATO position) and other layers as well (SDNS also provides a protocol for the Transport Layer).

Work has already begun on OSI services and protocols in the management area. Systems management is generally acknowledged to affect all service areas, especially operating system services and network services. The only consensus achieved to date for standardizing systems management services is in the OSI network management area. Version 1 (June 1992) of the GNMP identifies information required for managing implementations incorporating network services only at the Physical and Data Link Layers, and it does not provide a complete set of managed object definitions or the necessary security features for network management.

Support for access control and authentication is already being incorporated into a number of OSI standards. Many other aspects of security, such as key management, still must be

standardized to ensure interoperability and to avoid building the same functions many times in similar systems (e.g., function-specific information systems) and in the applications of a single system, such as a CCIS.

Management issues can be expected to differ for each of the technologies being considered for information systems. For example, security aspects of local area networks differ from those associated with broadcast radio and packet-switched point-to-point links.

Some issues and findings in security and OSI management are:

- Standards for OSI security are evolving, but the evolution is slow. OSI standards may not be satisfactory in some areas (e.g., OSI services) in and of themselves for military applications. They may need to be supplemented by application-level services outside the OSI model.
- An adequate treatment of management services may require modification to the OSI Basic Reference Model and thereby impact many stable OSI standards.
- Some management standards are now stable (e.g., ISO 9595, ISO 9596; ISO 10040, ISO 10164, ISO 10165), but there is standardization required in many additional areas.

13. DISTRIBUTED COMPUTING SERVICES

Quick Reference	
Topic	Page
APPN	306
Assessment	307
Client/Server	296
CORBA	301
DCE	302
Decision Support	305
Dist. Interactive Sim.	296
DME	303
Knowledge Engineer.	305
Middleware	304
MOM	304
NIIT	306
ODP	297
OMG	301
OSF	302
Requirements	296

This chapter addresses standards for distributed computing services. It describes the new IEEE standard for Distributed Interactive Simulation (DIS) Protocol Data Units (PDU), the ISO standard for Open Distributed Processing (ODP), the Object Management Group's (OMG) work, the Open Software Foundation's (OSF's) work on a Distributed Computing Environment (DCE) and Distributed Management Environment (DME), the Message-Oriented Middleware Consortium's (MOM) work, the National Information Infrastructure Testbed (NIIT) and IBM's Applications Peer-to-Peer Network (APPN) protocol. Distributed Transaction Processing (TP) is discussed with network service standards in Chapter 9 (Section 9.11.9). Management of distributed data and other information resources is discussed in Chapter 6 on Data Management Services.

Application Layer standards often define, at least partially, distributed services. Examples are Message Handling System (MHS), Remote Procedure Call (RPC), Directory, and File Transfer, Access, and Manipulation (FTAM); specifically, Directory contains a specification of a Directory Information Tree (DIT) and its associated navigation rules. The nodes of the DIT for ITU-TS are envisioned to be distributed worldwide. Such standards contain elements that relate to features (and models) of distributed applications and services, in addition to features related to data transfer.

General trends towards providing distributed systems functionality are through a set of servers—the predominant interaction model is the client-server. The term *middleware* is increasingly being used to describe the software that implements client-server connectivity. Two principal approaches are used: RPC and message-passing systems. [Ref. RNLA 1994, p. 26]

Object-orientation appears to be developing into a critical generic technology for distributed systems. Open operating systems are increasingly seen as a collection of interacting objects, with the objects themselves—representing the operating system shared services—being spread across a distributed system. Further, objects are being used as parts of models of the "real world" that a particular distributed computing system is controlling. Finally, objects are used to represent the shared services of a distributed system, hiding, for example, the details of legacy systems by enclosing them in wrappers. The latter view is especially important in the standardization of services for information systems. [Ref. RNLA 1994, p. 49]

The following are examples of tasks being proposed in generic work on distributed applications [Ref. IST/21: 1721 1989; SC21 N 4520 1990]:

- Model the information held by distributed applications and address the issues of distribution and local transparency (the ODP work has chosen to recognize five different viewpoints from which various features of a distributed application can be modelled); *Modelling for Communications Aspects of Distributed Applications* had been accepted by JTC1 and assigned to SC21/WG6. [Ref. SC21 N 4911 1990] However, WG6 has recommended that the project be deleted from the program of work since it lacks an editor and target dates and has been inactive.

- Formalize management interactions between application processes in specific protocols in such functions as establishing relationships, distributing data, and replicating data.
- Devise global security mechanisms for use throughout the entire domain of the distributed application.
- Enable the schema for information held at an applications process to be distributed among cooperating systems.
- Address database issues such as data integrity and consistency, together with replication of data.
- Identify constraints on process decomposition and interaction types (communication among subprocesses).
- Specify distributed application support for configuration management, reconfiguration, and routing.
- Define application features to allow migration for future extensions.
- Address real-time effects associated with distribution.
- Provide for time synchronization of application processes.

However, true distributed applications have yet to be achieved since the network is not hidden. A promising tool in this area is the RPC tool (see Section 9.11.3.5), which allows applications at run-time to move from one transport, such as TCP/IP, to another such as OSI. [Ref. OSN 1990c]

Within IEEE, the Distributed Services Steering Committee has oversight and coordination of all distributed services working groups.

13.1 Distributed Computing Requirements and Services

13.1.1 Requirements for Distributed Computing

Data Management. Data management requirements for distributed information systems, derived from ISO 10032, *Reference Model on Data Management,* are defined in Section 6.1.2.

Client/Server Capabilities. Distributed information systems will make use of client/server capabilities, and these capabilities are the subjects of many emerging standards. The Programming Language SQL (ISO 9075:1992) introduced the terms client and server as a basis for distinguishing capabilities of an SQL implementation, and the current standard for SQL specialization for remote database access (RDA) uses the terms client and server for communicating components that support access from an application process to a remote SQL implementation. There are alternative ways in which these capabilities may be combined and these may need to be standardized. For example, access to a remote IRDS can use either an RDA-based communication or a remote procedure call (RPC)-based communication. In addition, ODP (see Section 13.2) and many recommendations on distributed computing environments (see Sections 13.3 to 13.5) adopt the client/server paradigm. SC21/WG3 has proposed a question (Q3/011) on harmonization of client/server capabilities, which would address requirements for client/server capabilities, need for a client/server architecture, and potential use of such an architecture in SC21 standardization activities. [Ref. SC21 N 8019 1993]

13.1.2 Distributed Interactive Simulation (DIS)

A standard on Distributed Interactive Simulation (DIS) Protocol Data Units (PDUs) was developed by the DIS workshops and transmitted to the IEEE for standardization. It deals with application protocols for distributed simulation of battlefield entities that are controlled by humans

and operating in real time. Information such as type of weapons platform, country of origin, position, velocity vector, munitions and fuel status, etc., are described by the PDU. The PDU is the sole method of coordinating interacting entities. This standard was approved in March 1993.

Current work is in developing an augmented standard in which environmental effects and electronic warfare are more fully described. Version 2 is ready for submission and the group is ready to begin. An even greater variety of environmental and unit representation will be available in Version 3.

Companion standards for terrain and other common environmental databases are in early versions ready for submission to the IEEE. A communication profile for the use of those transmitting the PDUs between distributed hosts is also ready for submission in late 1993. A document describing exercise control and feedback requirements is in preparation for submission in 1994. A document concerning fidelity is due in late 1994.

13.2 Open Distributed Processing (ODP) Standards

Open Distributed Processing (ODP) allows both users and applications to interact remotely with any other computational resources (including other applications) held at different locations. A single application might also be divided into sub-units for execution in parallel on a number of machines linked together by a network. In its most sophisticated form, this allows multiple "clients" (users or their local applications) to request services from multiple remote "servers" using various software protocols such as a Remote Procedure Call (RPC) to achieve the required communications and synchronization. [Ref. OSN 1991j]

13.2.1 ODP Standards

ODP is a new area of standards development. Begun in 1987, the work has progressed so far in ISO that a new working group (SC21/WG7) was formed by the JTC1 to progress the standards for an ODP Reference Model. Moreover, ODP was added to the SC21 title in 1993. The current work comprises the framework of abstractions (e.g., the nature of the different points of view of a system); functions and interfaces; and modelling. It addresses the following aspects:

- Modelling distributed processing in terms of components, the services they support, their environment, and the interactions between them
- Identifying levels of abstraction at which the services and interactions can be described
- Classifying the boundaries between components and identifying the points of interaction associated with them
- Identifying generic functions performed by distributed systems
- Showing how the elements of the model can be combined to achieve ODP.

The *Basic Reference Model of ODP* (CD 10746) further defines levels of abstraction at which services and interactions can be defined in other standards, generalizing the concepts of service and protocol defined in the OSI Reference Model (ISO 7498). The structure of the Basic Reference Model is as follows:

- WD 10746-1 (Part 1): *Overview and Guide to Use,* containing a motivational overview of ODP, giving the scope, explaining the key definitions (with no substantial architectural content), and enumerating required areas of standardization (not normative)—CD is expected July 1994, DIS in January 1995, and IS in October 1996. Initiation of ITU-TS ballot approval is expected in 1996. The most recent WD is SC21 N 8218, September 1993.

- CD 10746-2.3 (Part 2): *Descriptive Model,* defining the concepts, analytical framework, and notation for normalized description of (arbitrary) distributed processing systems (not normative but establishes requirements for new specification techniques)—Currently in third CD (10746-2.3) [SC21 N 7988, August 1993]. DIS is expected in February 1994 and IS in November 1995. Initiation of ITU-TS ballot approval is expected in June 1995.
- CD 10746-3.2 (Part 3): *Prescriptive Model*, specifying the required characteristics that qualify distributed processing as open—these are the constraints to which ODP standards must conform—This major revision of Part 3 has added a set of viewpoint languages that can be used to define an ODP system. [Ref. OSN 1992m] (ITU-TS X.903) Currently in second CD [SC21 N 8125, August 1993]. DIS is expected in February 1994 and IS in November 1995. Initiation of ITU-TS ballot approval is expected in June 1995.
- WD 10746-4 (Part 4): The original Part 4, *User Requirements*, was merged with Part 1 in June 1992 since there was no major distinction between them and a danger of duplication [Ref. OSN 1992m]. Part 5, *Architectural Semantics* (originally entitled, *Architectural Semantics for FDTs),* is now Part 4—CD text is expected July 1994, DIS in January 1995, and IS in October 1996. Initiation of ITU-TS ballot approval is expected in 1996.

Principles for the specification of management for ODP systems are now being integrated into Parts 1 and 3 of the ODP standard.

13.2.2 Relation of [illegible] to Distributed Database Systems

SC21/WG3 has proposed a question on the use of ODP for distributed database systems (see Section 6.1.4). The basis for the question is the need to fit distributed database standardization into the broader context of a framework for distributed systems. Specifically, requirements for distributed database systems include several requirements related to distribution transparencies described in the ODP Reference Model: location, fragmentation, and replication of data; and the way data management services may be distributed to support these requirements. Work on the new question would address such issues as how the ODP Reference Model can be used to provide an architecture for the description of processing relevant to distributed database systems, which distributed processing functions can be used to support requirements of distributed database systems, what additional functions are required, and in what ways such functions require support of data management services. [Ref. SC21/WG3 N 1557 Rev 1993]

13.2.3 ODP Specification Techniques

Use of Specification Techniques in ODP is a new draft technical report split off from earlier work on CD 10746. This technical report defines requirements on specification techniques for ODP and evaluates standardized formal description techniques (FDTs) against these requirements. The formalization of modelling concepts, provided by a mapping to the concepts of each FDT, acts as a bridge between the ODP architecture and FDTs.

ISO/ITU-TS Joint Modelling Group has proposed the abstract specification language Z as a candidate FDT for use in ODP [SC21 N 6088]. In January 1992, a proposal for a new question (Q7/1) on the suitability of the FDT Z for use in ODP was accepted [SC21 N 6674]. The proposed draft answer to Q7/1 states that conventional Z meets many, but not all of ODP requirements. However, it is amenable to extensions to include object-oriented concepts, which many meet most of ODP requirements. Therefore, should a NWI on the standardization of Z be accepted, object-oriented extensions will be necessary. [Ref. SC21 N 7051 1992] The Trader Rapporteur Group

has agreed to adopt the Z notation for use in the information specification of the ODP Trader, specifically the formalization of the information objects and their relations. [Ref. SC21/WG7 N 737 1992

ODP Standardization Activities. The approach of SC21/WG7 has been to identify and expand a number of ODP topics in parallel. The applicable documents are:

- *Topics List—November 1989 Version—for the Basic Reference Model of Open Distributed Processing,* December 1989 [SC21 N 4019]
  - Topic 1—The Problem of Distributed Processing, March 1988 [SC21 N 2507]
  - Topic 2.2—Properties and Design Freedoms, December 1988 [SC21 N 3288]
  - Topic 2.3—Framework of Abstractions, December 1988 [SC21 N 3194]
  - Topic 3—Structure of ODP Standards, March 1988 [SC21 N 2509]
  - Topic 4.1—Functions and Interfaces, December 1989 [SC21 N 4022]
  - Topic 4.3—Function and Interface Definitions [SC21 N 6081]
  - Topic 5.1—Modelling Techniques and Their Use in ODP, December 1989 [SC21 N 4023]
  - Topic 6.2—Formalisms and Specification, December 1989 [SC21 N 4024]
  - Topic 7.1—Basic RM of ODP, December 1989 [SC21 N 4029]
  - Topic 8.1—Draft Basic RM of ODP, Part II, December 1989 [SC21 N 4025]
  - Topic 9.1—ODP Trader, June 1992 [SC21 N 7047]
- *List of Open and Resolved Issues—June 1992 Version,* June 1992 [SC21 N 7057]. The open issues are:
  - Issue 2: What should the working definition of ODP System be?
  - Issue 7: How is the conceptual schema communicated?
  - Issue 11: What should the human interface function be?
  - Issue 17: What are the principle abstractions associated with each of the five viewpoints?
  - Issue 23: What is the scope of an ODP enterprise?
  - Issue 24: What is the WG7 position on modelling, specification use, and roles of conceptual schemas?
  - Issue 25: How should translations from ASN.1 to ODP/DAF-selected FDTs be developed and should WG7 undertake this task?
  - Issue 26: Is the notion of event needed in basic concepts of Part 2?
  - Issue 27: What are the relationships between interface, interaction point, and binding?
  - Issue 28: What are the definitions of behavioral compatibility and refinement?
  - Issue 29: Are data elements objects?
  - Issue 30: Can alternative definitions for a function be given within a single viewpoint?
  - Issue 31: Is the initiate operation part of the trading function?

In November 1990, Australia proposed a new work item to develop a standard entitled: *ODP Trader — A Standard to Define the Role and Function of the Trader in Open Distributed Processing (ODP)* [ISO/IEC JTC1/SC21 N 5564, January 1991]. This NWI was accepted into the JTC1 work program in April 1992. The most recent WD on ODP Trader is SC21 N 8192 dated August 1993. CD text is expected in July 1994, DIS in December 1995, and IS in July 1997. Initiation of ITU-TS ballot approval is expected in 1996. The Trader is a component of an ODP system that supports trading interactions (a trader is defined to be an object to which an exporting object can advertise its services and from which an importing object can find its needs from the set of advertised service offers in a distributed environment). [Ref. SC21/WG7 N 783 1993]. The

document will include a normative annex on use of Directory. The ODP Trader standard is needed to ensure [Ref. SC21 N 6085 1991]:

- Portability of applications in an ODP environment
- Internetworking between ODP systems
- Distribution transparency in ODP systems.

The following lists, in priority order, the Trader work plan [Ref. SC21/WG7 N 737 1992]:

- Information specification of the Trader
  - Administrative control over construction and assessment of trading context structure (search policies, use of QoS in search policies, context membership rules)
  - Matching rules
  - Selection criteria
  - Z specification
- Computational specification of the Trader
  - Operation Definitions
  - IDL specification of operations and parameters
  - Specification of behavior
  - Naming of service types, trading context, service offers
- Issues in Enterprise Specification
  - Federating with Federation - the significance of uplinking and downlinking
- Conformance statements
- Relationship to X.500 and WG3 Database Management
- Relationship of Trader to other components
  - Type Management
  - Security Model
  - Accounting Model.

A recent WG7 working document (SC21/WG1 N 1253, May 1993) discusses the issues involved in specifying the QoS (see Section 12.1.6) so that they can be used in trading services (ODP Trader).

In the absence of an Editor and progression of the WD, an ODP project, *Use of Specification Techniques in ODP Semantics,* is under reassessment by SC21. [Ref. SC21 N 7728 1993]

Further, SC21 has proposed a new question on the relationship between the OSI Upper Layer Architecture (ULA, see Chapter 9) and ODP. This question has been accepted into the JTC1 work program [SC21 N 6609, 6 December 1991]. The draft answer states that ODP and OSI upper layers modelling activities differ in their respective scopes. While the RM-ODP provides a framework for the standardization of all aspects of distributed processing systems, the OSI Application Layer Structure addresses the modelling needs of distributed applications from a communications perspective. [Ref. SC21 N 6972 1992]

ITU-TS Group VII has proposed a question (Q16/VII) for the 1993-1996 Study Period that would continue the work of Q19/VII in the area of ODP. The question asks what new Recommendations are needed to [Ref. SC21 N 6956 1992]:

- Establish a set of modelling concepts to support a RM-ODP
- Detail the RM-ODP
- Specify an ODP Trader for use by ITU-TS applications.

In June 1992, a new question (Q1/66) on ODP Conformance Testing Methodology was proposed. Specifically, if focuses on what needs to be done to develop an ODP conformance testing methodology in ISO/IEC 9646 building on the concepts of ODP conformance described in the ODP Basic Reference Model. [Ref. SC21 N 7088 1992] The results of the ballot indicate that the majority of the National Bodies voting support work on the proposed new question. WG1 began work in June 1993. [Ref. SC21 N 7476 1992]

13.3 Object Management Group (OMG)

The Object Management Group (OMG) (see Appendix F) is a consortium of over 340 companies, educational institutions and governmental organizations that wish to establish de facto standards for the use of an object-oriented model of distributed computing. The group issues requests for technology based on specifications that its working groups develop.

The OMG does not develop products other than specifications. To date the OMG has issued an Object Architecture Guide and a specification for the Common Object Request Broker Architecture (CORBA), which is currently in Version 1.1. Products using or based on CORBA are now available, and OMG is developing a CORBA catalog of vendor implementations and applications using CORBA. [Ref. Stone 1993]

CORBA is one part of the Object Management Architecture (OMA) defined by the OMG. CORBA specifies the concept Object Request Brokers (ORB), which defines how a set of interworking classes and instances interact. An ORB provides an infrastructure allowing objects to communicate, independent of the specific platforms and techniques used to implement the addressed objects, guaranteeing interoperability of objects over a network of non-homogeneous systems. Together with Object Services, Common Facilities, and Application Objects, the ORB forms one of the four major parts of an OMA. COBRA includes a core communications infrastructure and a set of Object Adapters for different object implementations. COBRA permits client access services and object-references to be realized either through stubs generated from an interface definition language or through a dynamic API. [Ref. RNLA 1994, pp. 34-42]

A second revision of CORBA (2.0) to fix problems of interoperability and interface repository federation is underway. Currently, only a C mapping to the Object Request Broker (ORB) is specified. A C++ mapping is about to be selected; Smalltalk and COBOL mappings will be selected next year, as will an upgraded interface repository interface. The ISO ODP group is working to progress this work in their committee as a basis for their standards.

OMG is working on a revision of the Object Model document based on its experience with the ORB. It currently has issued a request for proposal on a collection of Object Services to be used with the ORB and a roadmap for the implementation of these services.

During the last half of 1993, OMG planned to procure life-cycle, naming, persistence, and event notification services. In the first half of 1994, OMG wants to procure relationship, transactions, and concurrency control services. In the last half of 1994, OMG wants to procure two packages of services. The first package includes security service, "exteriorization," data interchange, licensing service, and trading service. The second package includes query, change management, and properties services.

Additional services are specified in the Object Services Architecture. These services fall into two categories: (1) CORBA-related services, which include the interface repository and the implementation repository, and (2) system-related services. The Object Services Task Force

(OSTF) feels that the CORBA-related services will be dealt with by either the ORB 2 Task Force or the OSTF. The set of system related services were not of the highest priority but may be dealt with by OSTF at a later time. They include such services as archive, backup, startup, installation and activation, operational control, replication, object threads, and time.

OSF, UI, and X/Open all have endorsed the OMG and its ORB in particular. OSF and UI plan to provide a version of the ORB in the "near future." Hyperdesk and Hewlett Packard offer ORB toolkits today. In February 1993, the OMG requested a liaison with ISO/IEC JTC1 SC21/WG7. [Ref. SC21 N 7613 1993] The SC21 response was favorable and included a paper [Ref. SC21 N 8034 1993] that compares ODP and OMG architectures. The goal of the paper was to serve as a basis for converging the two architectures so that the OMG specifications can become potential candidates for fast-track adoption by ISO, to fulfill the requirements for ODP functions as identified in ODP-RM-3 (CD 10746-3). Potential candidates for early use in ODP included in the comparison were COBRA, persistence, life-cycle service, event service, and name service. Candidates for later use in ODP were transaction, concurrency control, time, relationships, and externalization services.

13.4 Open Software Foundation (OSF)

The Open Software Foundation (see also 15.1.2.4 and Appendix F) is a consortium of over 360 members including commercial, government, and university groups. It is a technology integrator and distributor of Open Systems Technology with over 300 employees worldwide. Its technology products include an operating system, OSF/1 Release 1.2 (see Section 10.2.2); a visual user interface and toolkit, Motif 1.2 (see Section 5.2.7); and a distributed computing environment, DCE 1.0.2A. Products in progress include components of a distributed management environment (DME). Research at the OSF Research Institute is leading to a neutral distribution format (ANDF) methodology (see Section 15.1.3.5) for distributing portable software and a microkernel (Mach) (see Section 10.2.2) on which later versions of UNIX can be based.

13.4.1 Distributed Computing Environment (DCE)

The OSF DCE[73] contains a number of subsystems designed to extend UNIX functionality. The reference version of DCE is available for OSF/1. User-contributed versions are available for UNIX SVR4 (from Siemens). (Note: clients for the PC have been done by Gradient Technology for Windows and by IBM for OS/2 Release 2.x). Versions are also available from manufacturers running on a wide variety of platforms and operating systems. DCE provides the following:

- A threads library. This library permits the development of multi-threaded applications, essential to development of servers. According to OSF, this library corresponds to POSIX P1003.4a (draft 4).
- A remote procedure call facility and toolkit based on work of Hewlett-Packard (HP) and Apollo's NCS version of remote procedure call (RPC). This is the mechanism that permits authenticated interaction between heterogeneous, distributed client programs and server programs.
- A network time protocol (NTP) developed by Digital Equipment. This provides a provable, bounded time over an arbitrary network. It is a requirement for the authentication scheme used in DCE.

---

[73] OSF DCE is a trademark of the Open Software Foundation, Inc.

- An authentication service based on Kerberos 5.0 from the Athena project at MIT and improved by Hewlett Packard. This service provides certification of identity to those services that require it.
- A scaleable set of distributed file services derived from the Carnegie Mellon University ANDREW project and commercialized by the TRANSARC Corporation. This file system is designed to run with a satisfactory performance over wide area networks (WANs).
- Directory services, including a local directory service for the smallest administrative level or cell level (CDS) provided by Digital Equipment and a global directory service compatible with the X.500 standard provided by Siemens. These services allow transparent file reference across multiple distributed, heterogeneous platforms.
- A product permitting distributed transaction based computing based on the Camelot transaction system from Carnegie Mellon University and commercialized by TRANSARC Corporation under the name ENCINA.
- A set of products promoting PC integration including Microsoft's LAN Manager and Locus' PC Interface program.

OSF's DCE has been widely implemented or is in the plan of most major manufacturers of Open Systems. It is installed in over 1,200 sites. OSF has compiled a catalog of more than 70 products, including DCE implementations as well as DCE-enabled tools and applications. The bulk of these products are currently available, with the rest planned for 1994 delivery. DCE has been accepted by X/Open and UNIX International, de-facto standard setters for industrial open systems. It will form part of the base for COSE.

13.4.2 Distributed Management Environment (DME)

The DME is designed to be layered on top of DCE regardless of the manufacturer or system software. It consists of a number of parts to be delivered in three phases. Phase 1 consists of a Software Distribution Service (SDS), License Management Service (LMS), Event Service (EVS), Subsystem Management Service (SMS), and PC Services (PCS). Phase 2 consists of a Print Management Service (PRS). Phase 3 consists of a management framework.

Phase 1 of DME. The software distribution service provides for the delivery, maintenance, and update of software using network resources. This is particularly useful in large environments. The original technologies were from HP and IBM.

The license management service will provide a standard infrastructure that will permit software to be used on a license available basis. In this practice, a pool of licenses is established for the cell. Individual licenses may be obtained from the pool by any authorized user. Presentation of the license gains use of the software. When the use of the software is finished, the license may be made available for another user. The original components were from HP and Gradient Technologies.

The event service makes possible the communication of network and system events to users on other parts of the distributed computing resource. Emergencies such as paper outage, requests such as for media mounting, and announcements such as routine maintenance schedules may be handled uniformly by the event service. The original technologies were from Wang Labs.

Subsystem management service permits a user to administer individual components of the cell from authorized locations in the physical network, and to manage heterogeneous systems a uniform manner. For example, platforms and servers may be started or shutdown.

PC Services permit invocation of and communication with services available in the computing environment from an MS-DOS machine and use the minimal resources. These components were developed by Gradient Technologies. Phase 1 began shipping as of mid-November 1993 as DME 1.0.

Phase 2 of DME: Print Services. The print services are used by management and user applications to print and control the use of printing resources. The printer supervisor and spooler use the ISO 10175 DPA protocol. The printing systems program interface is used as the base for the POSIX printing management standard. These components were originated at Project Athena at MIT and adapted by DEC. Delivery is expected in the second quarter of 1994.

Phase 3 of DME: The Management Framework. The management framework is most comprehensive. Originally provided by Tivoli Systems and Bull, S.A. of France, this framework was to have managed network assets utilizing SNMP and TCP/IP protocols as well as CMIP and OSI protocols in a manner transparent to the user. With the advent of the Object Management Group's Common Object Request Broker, the management framework was recast to use the new technology with IBM's help in rewriting the Tivoli interfaces. A standard user interface for management applications is also provided.

13.5 Other Distributed System Standardization Initiatives

13.5.1 Message-Oriented Middleware Consortium (MOM)

The Message-Oriented Middleware Consortium (MOM) [Ref. Stahl 1993] is a new middleware-vendor association. MOM promotes middleware that uses messaging technology to allow applications to communicate across distributed platforms. Consortium members include Digital Equipment, IBM, and Covia Technologies.

Middleware has been variously defined as:

- Technology that shields applications from underlying network protocols and operating systems;
- Technology that allows users to access multiple databases without knowing the intricacies of each; and
- Software that sits between client and server in a distributed computing environment.

There are several types of middleware including application programming interfaces (APIs) (see Section 15.2), remote procedure calls (RPC) (see Section 9.11.3.5), network messaging (see Section 9.11.4), database access (see Section 6.2.2.2), and computer-aided software engineering (CASE) tools (see Section 4.3.2). The intent of the consortium is to create standards in messaging middleware.

13.5.2 Multinational Projects in Europe

In parallel to various industry initiatives in distributed systems, such as DCE and COBRA, there has been considerable effort spent on distributed systems. These include the following (in Europe) [Ref. RNLA 1994, pp. 51-52]:

- Advanced Networked Systems Architecture (ANSA)—initiated as an Alvey project in the United Kingdom and continued in the ESPIRIT project ISA. ANSA defines several aspects of a distributed object-based architecture, including a computational model (the fundamental object model), a naming model (for naming objects in a distributed system), a model for interface groups (for object replication), an engineering model (with proposed implementation structures), an approach to currency control, a programming language, and a (partial) implementation.

- ESPIRIT ISA—promotes ISO ODP and has developed an evaluation chassis (AnsaWare) for ODP. AnsaWare is not yet directly compatible with OSF's DCE or DME, UI Atlas, or COBRA.
- ESPRIT COMMANDOS (now inactive)—investigated tools and services for an advanced object-based distribution platform, including database integration, which led to a number of prototypes.
- ESPIRIT Harness—merges technology results into a common architecture and a prototype, with the goal of integration with a DCE snapshot.
- ASSET—a project (Advanced System and Software Engineering Enabling Technologies) of Bull, Olivetti, and Siemens-Nixdorf, with a goal of establishing a European Development Environment for Open Distributed Systems based on COBRA and results from COMMANDOS and ISA/Harness.
- Eureka Software Factory (ESF)—a project to make a factory environment for developing software that is adaptable to different organizations and application areas, carried out by a consortium of 14 different companies in five European countries. ESF is based on a "software bus" that defines interactions among software components (much as a hardware bus does for hardware components) and provides a unique global environment by encapsulating heterogeneous, interoperating systems within a common interface. Its work has addressed control integration (software bus), presentation integration (user interface building tools), data integration (object storage services), and work-process integration (process modelling support):
- CADDIE—a software environment supporting design and implementation of dynamic and distributed multi-agent decision systems and control hierarchies with an open architecture based on object-oriented design and intended to conform to emerging standards in object-oriented programming and knowledge representation. One of the largest multi-agent systems developed to date using commercially available tools, CADDIE was partially funded by the UK Department of Trade and Industry.

13.5.3 Decision Support and Knowledge Engineering

Decision Support Architectures. A promising architecture for decision support systems is a multi-agent architecture based on a blackboard data structure, whose key components are the agents and the blackboards. Agents are composed of knowledge sources that contain information about a specific action the agent can perform. A control mechanism is needed in order to carry out the planning process, since several agents can execute simultaneously trying to achieve different goals. Such agents communicate with each other using the blackboards. More than one planner method (strip or hierarchical) can be implemented with this architecture. Use of the blackboard data structure allows a neat implementation of the events as simple changes in the objects of the blackboard. Support of concurrent operations from a multitasking operating system and use of real-time tasking services is desired. These would support the range of tasks, both periodic and nonperiodic, associated with C3I applications, with time deadlines working concurrently within the system and with large amounts of incoming data that needs to be processed quickly. [Ref. RNLA 1994, pp. 286-287]

Advanced Technology Operations System (ATOS). ATOS uses results of the DARPA Knowledge Sharing Effort (e.g., Knowledge Query and Manipulation Language and Knowledge Interchange Format) to specify communications between applications with respect to a shared model (ontology), which defines concepts and terms that the applications use to exchange domain information. Work on ATOS is being carried out by a consortium consisting of Logica Space, Communications Limited, Space Application Services, and GMV. It addresses

development of mechanisms to enable translation between knowledge bases represented in different languages, common versions of languages within families of representation paradigms, protocols for communication between knowledge-based modules, and libraries of ontologies that contain skeletal application-specific knowledge bases in particular domains. [Ref. RNLA 1994]

ATOME-TR. ATOME-TR is a project that provides a development environment for prototyping complex applications as a parallel "blackboard" system on a single processor workstation. In the blackboard model, three types of agents interact: the strategy knowledge source that coordinates the overall activity of the system, the task knowledge sources that coordinate local activities, and the specialist domain knowledge sources that infer hypotheses in the blackboards. ATOME-TR implements a real-time control model based on reactive planning in order to control all the agents according to temporal deadlines and to implement approximate or progressive reasoning with real-time constraints. This project is conducted by a consortium of Matra Defense, Matra Cap Systemes, and CRIN/INRIA Lorraine research laboratory in France, with support from the French MOD (DRET) and the French Ministry of Research and Technology. [Ref. RNLA 1994]

13.5.4 National Information Infrastructure Testbed (NIIT)

The National Information Infrastructure Testbed (NIIT) is a consortium of representatives from US industry, academia, and government that was formed in September 1993 to leverage the National Information Infrastructure (NII) vision and principles. NIIT will implement the vision of the NII through the development of distributed applications requiring the speed and transmission capacity of a true data superhighway system. Digital is among the members of the NIIT, which will be standards based. [Ref. OSS 1993]

13.5.5 Applications Peer-to-Peer Network (APPN)

Cisco, Founder of the APPI (Applications Peer-to-Peer Interface) Forum has recently shifted its efforts away from APPI, which was to network IBM systems over the Internet's IP protocol and has licensed IBM's APPN peer-to-peer networking protocol. Although the APPI goal was technically feasible, to build it without use of IBM-patented technology would require "work-arounds" that would not have enough functionality to fulfill users' needs. Cisco claims that APPI has nevertheless forced IBM into dealing more openly with the industry. IBM has set up an APPI Implementor's Workshop (AIW), which shares developments with users and vendors, published the APPN specifications, and licensed the patents. [Ref. OSN 1993s]

13.5.6 System Object Model (SOM)

IBM has used a System Object Model (SOM) as the basis of its emerging distributed object computing environment. SOM permits objects to be defined using a variety of languages, using a common binary format for object classes that will be shared, and providing bindings to C and C++. SOM also allows object-oriented software to be packaged and shipped as binary object class libraries (e.g., it allows object classes to be packaged for Windows and OS/2 and as shared libraries for AIX). SOM is both an architecture, defined by an API, and a runtime environment. SOM includes a COBRA-compliant interface definition language (IDL) compiler used to write class declarations; a call-level API; language bindings for C and C++; base classes; an interface repository, which is a framework to provide runtime access to all information contained in the IDL description of a class; and Distributed SOM (DSOM), which is a framework that supports transparent access to remote objects and which supports both the static and dynamic COBRA

APIs. DSOM is an extensible ORB, permitting developers to add their own methods. Currently, DSOM interfaces to communications services using Berkeley Sockets and supports TCP/IP on AIX; and TCP/IP, NetBIOS, and IPX on OS/2. Future versions of SOM are planned to work with the DCE and make use of the DCE RPC, its location service, and its security service. [Ref. RNLA 1994, pp. 42-43]

13.6 Assessment of Open Distributed Computing

The effort that OSF has put into DCE is beginning to mature. The technology will be widely available in the first half of 1994. Most major open systems vendors will offer a version interoperable with the others on their UNIX-based systems. Many will also feature DCE ports on their proprietary systems, for example IBM's OS/2. SUN and Microsoft may be the only exceptions; however TRANSARC will provide a version for Solaris and Gradient Technologies will provide a version for Microsoft Windows.

In terms of de facto standardization, UNIX International has promised to provide DCE compatibility in the near future; Siemens already provides a SVR4 version of DCE as an OSF Reference Model. X/Open is "fast-tracking" DCE for incorporation into its next version of XPG. After being "standardized" by X/Open and adopted by the open system vendors, actual ISO or ANSI standardization is expected.

The current version of DCE appears to be usable for unclassified purposes. Care must be exercised if it is to be used for classified purposes. The next year will see the definition of a generalized security API for DCE that will aid the implementor in developing applications that deal with classified data. Few applications utilizing DCE exist. Developer kits and the standardization of the application environment will help to provide the impetus so that applications using the interfaces should begin to appear late in 1994.

One of the most demanding application suites, the Distributed Management Environment 1.0 has just been released to vendors. DME must still be tailored to the DCEs of individual manufacturers. Printing services and their management will not be provided until the spring of 1994. The management framework is not due until late in 1994 or early in 1995. Complete management services based on an integrated set of services from DCE and DME are not likely until mid-1995 at the earliest.

Integration could be hastened if the deployment of the OMG Object Request Broker and dependent services is accelerated. Currently a number of manufacturers have ORB product available. The new version of the ORB that emphasizes interoperability is not yet available. One might expect its specification in 1994 with implementations in early 1995. The ORB and its associated suite of object services should be available in late 1995 or early 1996. These services, which could be based on DCE, could stimulate the development of distributed services and applications. If kept on track, DCE, DME, and the ORB should enable the high volume production of applications by 1997.

(This page intentionally left blank)

14. INTERNATIONALIZATION

Quick Reference	
Topic	Page
Assessment	310
ISO Activities	309

14.1 ISO Activities

ISO/IEC JTC1 SC22 established WG20 to examine issues pertaining to internationalization. Specifically, the role of WG20 is to "identify elements relevant to the work of SC22 that may be affected by differences in language, culture, customs and habits; for these elements, [to] develop standards that enable applications to be portable across differing cultural practices; [and to] develop a Technical Report that describes a framework for nations to provide those elements." [SC22 N1424]

To this end, WG20 has divided its work into three parts:

- Preparation of a Technical Report that addresses the problems that need to be addressed, and the tools and capabilities that programming languages need to provide, or support, in order to enable software to be internationalized. This report is intended to provide enough information to allow SC22 WGs to establish plans for the incorporation of internationalization facilities into their languages. It is expected to reach PDTR registration and ballot in mid 1994.
- Revision to TR 10176, *Guidelines for the Preparation of Programming Language Standards*. This revision will consist of additional new sections to the existing TR to address the particular problems of internationalization. It is expected to reach PDTR registration and ballot at end of 1994 or early 1995.
- Preparation of several international standards and registries, which will define tools and information sources that can be used by programming languages to provide specific internationalization functionalities.

Two existing standards that provide such tools are:

- ISO 10646-1, *Universal Multi-Octet Coded Character Set*
- ISO 8859-1, *8-bit Single-Byte Coded Graphic Character Sets, Part 1: Latin Alphabet No. 1.*

One standard currently being worked on is the international ordering standard for data stored in ISO 10646-1 facilities. This standard will provide a default international ordering mechanism. It will be built on a rich character set that allows adaptation to a specific code set by subsetting the reference repertoire through elimination of entries. Additional work is expected in the areas of:

- A specification standard for cultural conventions
- An API standard for internationalization
- A registration standard for cultural convention sets
- A standard for a modifiable ordering of IS 10646 repertoire strings
- A standard for the classification of IS 10646 repertoire characters.

ISO/IEC JTC1/SC21 is also investigating internationalization of directory services [SC21 N 7019]. A report has been distributed that discusses requirements for operating Directory services in multi-national, multi-lingual, and multi-cultural environments [SC21 N7931]. This report recommends that the Directory standard be enhanced to allow attributes and Directory operations to contain the concept of 'locale' and proposes a model for this enhancement. (Locale

refers to information that identifies end-user environment elements such as language, character set, and cultural preferences for items such as date and time display, punctuation, units, and so on.) Specific changes required in the Directory standard have not yet been identified.

14.2 Assessment

The character set work is the most mature. Some industry actions have also occurred. MKS has announced fully internationalized and multibyte-enabled versions of its InterOpen source code products. These are InterOpen/Multibyte POSIX shell and utilities, InterOpen/Multibyte SPG4 commands and utilities, and InterOpen/Multibyte XPG4 terminal interface. Single byte internalization allows text messages, input, output, and data processing to occur in most languages for which a single byte character set exists - such as French, English, and German. Multibyte internationalization extends this to accommodate large repertoire languages such as Japanese and Chinese, while maintaining support for single-byte languages. IBM is the first company to license the internationalized version of InterOpen/POSIX shell and utilities, and implements this source code on its mainframe operating system OpenEdition MVS.

15. APPLICATIONS AND APPLICATIONS PORTABILITY INTERFACES

15.1 Applications Portability

15.1.1 Requirements for Portability

Portability is a software attribute representing the ease and cost effectiveness with which that software and data can be used on heterogeneous hardware/software platforms. Three key determiners of portability are the operating system, database access, and applications software. Hardware environment changes that require change of the operating system are in many cases significant to portability. This aspect of application portability is addressed by enforcing a standard (POSIX) for an *interface* between the operating system and the application program.

The interoperability aspects of information exchange mean that information systems need to have a consistent way to record meanings and relationships of data, and to distribute and replicate the data and changes to the data. This leads to the need to standardize the data models (schema) for databases and the services for accessing those databases. SQL is an example of a standard for services supplied to applications that access databases conforming to a relational data model. Additional standards may need to be developed for other data models. Standards for development of applications software take the form of programming language standards, together with standard methods for using the programming language.

Following the guidelines and standards will improve the prospects of, but not guarantee, application portability. Many aspects of implementations of POSIX, SQL, and Ada environments are inherently hardware dependent. Further, the standards do not provide all the needed services. Use of nonstandard options available in the implementations of operating systems, SQL, and programming languages can greatly restrict portability.

15.1.2 Organizations Promoting Applications Portability

15.1.2.1 ISO

In April 1988, JTC1 of the ISO/IEC began a formal Joint Technical Study Group (TSG-1) for Applications Portability (JTAP). Managed directly under the JTC1, and not any of the subcommittees, the JTAP study addressed five areas: (1) concepts and definitions related to applications portability, (2) user requirements, (3) portability issues, (4) internationalization (to investigate the interface requirements of users with different cultural backgrounds) (see Chapter 14), and (5) a framework for interfaces for applications portability (IAP). The final report [Ref. JTAP 1991] contains 11 recommendations. It does not contain an explicit list of application portability standards as mentioned in the original mandate because such a list would comprise

almost all of the JTC1 projects and standards. The recommendations of the JTAP report are that JTC1 should do the following:

1. Instruct its standards groups to use the methods and concepts described in the report.
2. Establish channels of communication with groups outside JTC1 in order to assist them in developing, recording, and using application environment profiles.
3. Use application environment profiles to identify standards work needed.
4. Establish procedures for managing application environment profiles, taking both user requirements and TR 10000-1[74] into account.
5. Establish procedures for the coordination of the work on base standards and application environment profiles that may lead to the development of new standards.
6. Initiate work to develop a taxonomy for application portability.
7. Instruct all of its standards groups to implement the portability considerations of Annex A [to the JTAP report] ("Necessary Portability Considerations for all JTC1 Standards Development").
8. Publicize activities in relation to the development of standards relevant to application portability in order to increase user awareness and participation, and promote the early use of standards.
9. Solicit user needs and priorities when initiating and guiding work relevant to application portability.
10. Review its mechanisms for coping with subjects that span multiple subcommittees such as application portability, security, and internationalization (see Chapter 14).
11. Establish means (e.g., Special Group) for:
    - Interacting with user groups
    - Recording application environment profiles
    - Developing a taxonomy for application portability.

JTAP terminated on September 1991. As a result of the JTAP work, SC22 has initiated Working Group 20 on Internationalization (see Chapter 14). The Group will take the POSIX work as input to address the complex technical problem of porting applications across other languages and cultures. Likewise, ASC X3 has formed a new Technical Committee, X3T7 on Internationalization. The Japanese National Body has proposed the establishment of a new JTC1 subcommittee to be devoted entirely to application portability.

ISO has recognized that standardization is needed for information processing that goes beyond data communications services and protocols. As will be shown in the sections that follow, there are major efforts under way in the areas of standard interfaces to operating systems, databases, graphics, user input and display devices, and programming languages. In addition, open systems standards are being developed for document interchange and distributed processing.

SC21 has identified [Ref. SC21 N 3134 1988] the need to provide standardization in the following areas related to information system interoperability:

- Information exchange
- Internetworking of systems
- Specification of functions needed in systems built for specific purposes
- Portability of applications across system hardware and software

---

[74] TR 10000 is an ISO technical report by the Special Group on Functional Standardization (SGFS) detailing the framework and taxonomy for International Standardized Profiles (ISPs). See Section 16.1.2.

- Definition of common interfaces to system services
- Security of systems
- Reliability of systems
- Human-computer (man-machine) interfaces
- Definition of common concepts
- Safety and legal requirements.

SC21 specifically plans to address standardization for database management systems and single and distributed processing environments, in addition to open systems interconnection.

15.1.2.2 National Institute of Standards and Technology (NIST)

NIST has been working with the IEEE and other US organizations to identify environments for open systems that can be specified with existing OSI and other open system standards. The NIST recommendations are contained in the APP, which is discussed in Section 15.1.3.3.

15.1.2.3 X/Open

X/Open (see Section 2.3 and Appendix F) is a non-profit consortium developing a Common Applications Environment (CAE) to promote applications software portability. X/Open relies on the selection and adoption of de jure standards, implementing a policy of using these in preference to development of its own. It also works with other specialist consortia to develop specifications that help to accelerate the processes of standards development. The X/Open Portability Guide (XPG), now in Version 4 (XPG4) specifies the CAE. XPG4 represents a significant advance over previous editions in that about half of the XPG4 components relate directly to formal standards. Standards recommended for the CAE are discussed in Section 15.1.3.4.

X/Open has entered into an agreement to acquire the UNIX trademark from Novell (who purchased UNIX International in 1992). When finalized, the UNIX name will be used to brand systems that comply with the UNIX API (also called the Common OS API or 1170 API) developed by X/Open (see also Section 10.2.3). The UNIX API combines functions of SVR4, IBM's AIX, Hewlett Packard's HP-UX, and OSF's OSF/1. [Ref. OSN 1993q] Since no system currently complies with the whole 1170 specification, an interim agreement has been set up whereby suppliers can use the UNIX brand immediately if all of the following conditions are satisfied [OSN 1993r]:

- The system conforms to X/Open's XPG3 or 4 base, and the USL System V Interface Definition (SVID 2 or 3).
- The system is derived from USL operating system technology.
- The supplier has committed to delivering the 1170 API.

15.1.2.4 Open Software Foundation (OSF)

The Open Software Foundation (OSF) (see also Appendix F) is an international consortium of over 360 members including commercial, government, and university groups formed in May 1988 to promote applications portability. It is a technology integrator and distributor of Open Systems Technology with over 300 employees worldwide. Its technology products include an operating system, OSF/1 Release 1.2 (see Section 10.2.2); a visual user interface and toolkit, Motif 1.2 (see Section 5.2.7); and a distributed computing environment, DCE 1.0.2A (see

Section 13.4.1). Products in progress include components of a distributed management environment (DME) (see Section 13.4.2). Research at the OSF Research Institute is leading to an architecture neutral distribution format (ANDF) methodology (see Section 15.1.3.5) for distributing portable software and a microkernel (Mach) (see Section 10.2.2) on which later versions of UNIX can be based. Other standards recommended for OSF are identified in Section 15.1.3.5.

The role of OSF is to determine the user's requirements for a function; to request information on the availability of current products to satisfy that function; to select appropriate technology from vendors, securing the ability to license its offering to all at reasonable terms; to integrate the technology into a reference offering; and to distribute source code for the reference product to all licensees.

15.1.2.5 OIW Technical Committee on OSE (OSE-TC)

In 1991, the OIW changed its name from the OSI Implementor's Workshop to the OSE Implementor's Workshop. At the same time, it established a Technical Committee on OSE (OSE-TC). In December 1993, the OSE-TC formed five subcommittees to focus on specific issues being addressed by the OSE-TC. The committees are the following [Ref. Johnson 1994]:

- <u>Profiling Work/Issues Subcommittee</u>—Provides guidance on the development of user defined Open Systems Environment (OSE) profiles. Guidance will build on work done by the ISO/IEC JTC1/SGFS in ISO/IEC TR 10000-3, *Principles and Taxonomy for OSE Profiles* (OSE-TC/93-084) and the EWOS) document, *Method for Developing and Documenting OSE Profiles* (OSE-TC/93-064). Specifically the subcommittee will:
  - Define and prototype a user profile development methodology
  - Document and analyze the user profile development methodologies of the OIW SIGs such as the Desktop Environment SIG, Multimedia SIG, and Healthcare SIG.
  - Coordinate with ISO, OIW SIGs, other Regional Workshops (EWOS and AOW) and user organizations who have expressed an interest in developing OSE profiles.

  Work items will include the following: guide to profile writers on how to develop and document OSE profiles; prototype OSE profile(s); and input to ISO, OIW SIGs and other regional workshops on developing OSE profiles.
- <u>OSI and TCP/IP Convergence Subcommittee</u>—developed a strawman outline of convergence profiles that identified areas that require profiling and the profiles needed in each area; addressing federal/user group procurement mandates, Internet IP next generation (IP:ng), user/vendor profiles, catalog convergence and coexistence (CC) technology, and consensus CC strategies/architectures.
- <u>Electronic Commerce Subcommittee</u>—addresses proliferation of EDI conventions or implementation agreements covering the procurement related transaction sets and the technical issues involved in integration of EDI/EDIFACT with information technologies, to include the following:
  - Communications (OSI and Internet)
  - Security, privacy, non-repudiation
  - Electronic mail (OSI and Internet)
  - Multimedia
  - Database
  - Application programming interfaces

- Testing to be done for compliance with EDI standards
- EDI input and output option for applications software
- EDI enveloping implementation agreements for Internet and OSI protocols.

- Desk Top Sub-Committee—The Desktop Environment SIG addresses issues affecting the end users' interaction with their computing environment, a scope independent and complementary to the other OIW SIGs. Specifically, the SIG employs standards and publicly available specifications for protocols and interfaces to develop profiles to access functionality available from the desktop. Issues falling under this charter include standard desktop tools, graphical user interfaces, multimedia interfaces, object management, the coexistence and convergence of multiple environments, the transition from standalone systems to distributed environments, and the need for publicly available specifications of proprietary interfaces. The SIG determines which interfaces map to existing profiles and identify gaps within those profiles. Work items include the following:
  - Define and clarify the scope of the desktop environment and the SIG relationship to the other service areas identified by various profiling methodologies.
  - With the assistance of the OSE Technical Committee, assess the appropriateness of these methodologies for meeting identified user requirements for the desktop environments.
  - Develop a profile for end user access to multiple environments from a single device (personal computer or workstation).
  - Using established OIW procedures, identify the publicly available specifications and their reference implementations for standalone and distributed desktop environments.
  - Develop a profile for achieving user portability across different standalone desktop environments.
  - Identify appropriate transition methodologies for migration from single-user to distributed environments, independent of underlying hardware and operating system implementation.
  - Develop a profile for user portability across different distributed desktop environments, including those environments available from POSIX compliant vendors.
- Distributed Computing Sub-Committee—Addressing middleware (application support software) and other topics related to distributed computing standardization.

TCP/IP-OSI Convergence and Coexistence (CC). The NIST developed two papers addressing the convergence issue and distributed them to the December 1993 meeting of the OSE-TC: *Protocol Coexistence and Convergence* (OSE-TC/93-154), and *Functional Comparison of the Internet Protocol Suite and the OSI Protocol Suite* (OSE-TC/93-155).

Electronic Commerce (EC). In December 1993, the OSE-TC hosted a special session on Electronic Commerce with representatives from federal and state government, industry associations, and the electronic data interchange (EDI) standards organizations (DISA and ANSI X12). The key issue is the US Federal Government's requirement to start implementing Electronic Commerce by September 1994 (OSE-TC/93-171). In October 1993, President Clinton signed an Executive Memorandum to federal agency heads regarding electronic contracting (OSE-TC/93-132). However, the Federal EDI community has become concerned over the proliferation of EDI conventions or implementation agreements covering the procurement related transaction sets. This meeting provided the first forum for bringing together government users and industry associations to address these concerns and identify areas for cooperation and develop plans for implementing Electronic Commerce. Government users will identify requirements and provide this

information to DISA/ANSI X12 for identification/development of transaction/message set guidelines. The OSE-TC will develop a technical assessment of OSI, Internet and other protocols required to support Electronic Commerce. The assessment will also address government policy barriers to implementation. The EC subcommittee developed an action plan, scope of work, and objectives for the assessment to be presented at the next meeting (OSE-TC/93-195).

Public Windows Interface (PWI). Users and vendors have invested substantially in Microsoft Windows Applications and need an agreed standard for PWI. Both groups are concerned about the portability of applications and personnel to platforms with other graphical user interfaces. A draft PWI specification was developed by SUN, IBM, X/Open and others, which is not made up of any Microsoft code. The PWI provides a common application programming interface (API) for personal and productivity applications. PWI aims to ensure portability of these applications, as applications written in compliance with this API will run on any PWI-compliant desktop. The PWI specification will be submitted to major industry, national and international standards organizations for acceptance as a public standard.

National Standards System Network (NSSN). ANSI has obtained federal funding for the NSSN from the Technology Reinvestment Project (TRP). A team led by ANSI will develop an electronic network to link the heterogeneous databases of hundreds of organizations involved in the development, production, distribution, and use of technical standards in the United States. This electronic information infrastructure will reduce standards development time, minimize duplication of effort, and decrease production costs.

Protocol Independent Interfaces for Process-to-Process Communications. NIST is working on convergence APIs for Internet and OSI network process-to-process communications through the POSIX P1003.12 Committee. P1003.12 Draft 4.0 specifies a low-level Detailed Network Interface (DNI) that provides access to protocol-specific features of the underlying network. DNI consists of the X/Open Transport Interface (XTI) and the BSD Socket Interface (XTI does not provide access to the identical set of services as Sockets). The first ballot for 1003.12 closed in October 1993. Draft 4.0 includes two C bindings for DNI (XTI and Sockets), event management interface, language-independent interface mappings for protocol profiles, C binding interface mappings to protocols, and relationship between bindings and LIS. The focus is portability of applications between open networks. Applications that use XTI and Sockets can run over both OSI and Internet protocols.

15.1.2.6 Desktop Management Task Force (DMTF)

The DMTF is a supplier-led group that will develop specific de facto standards for managing elements within networked desktop systems. It was founded at the Spring 1992 Interop trade show by Microsoft, Novell, IBM, Digital Equipment, Hewlett-Packard, SunConnect, and Synoptics, and at least 150 members have joined since. DMTF's tasks are the following:

- Define a set of open APIs, called the Desktop Management Interface (DMI; see Section 15.1.3.10) for managing desktop systems
- Define a simple method of managing desktop components
- Distribute the specification and a reference implementation at no charge to hardware and software vendors.

DMTF hopes the result will be a set of rules for accessing multiple hardware and software components on a desktop computer consistently across multiple management platforms. The

interfaces between components, local agent, and management application are independent of any one operating system, network operating system, or protocol. [Ref. OSN 1993]

15.1.3 Standards for Applications Portability

This section discusses the standards recommended as profiles for applications portability. The areas addressed are interfaces for applications portability, NIST APP, UK MOD Model, X/Open CAE, OSF, the Technical and Office Protocol (TOP), Multivendor Integration Architecture (MIA), EWOS profiles for open system environments, UNIX International's ATLAS (UI-ATLAS), the Desktop Management Interface (DMI), and the SPIRIT (Service Providers Integrated Requirements for Information Technology) project. Several of the profiles discussed here and elsewhere are procurement profiles. The first procurement profile was General Motors' MAP protocols (see Section 9.11.5.1) , and perhaps the most powerful has been the government OSI profiles (GOSIPs) (see Section 16.1.3). Other profiles currently active include the NTT's MIA (see Section 15.1.3.7), and the Telcos' SPIRIT (see Section 15.1.3.11).

15.1.3.1 Interfaces for Applications Portability (IAP)

JTAP [Ref. JTAP 1991] examined the interfaces that need to be standardized in order to facilitate portability of applications. It concluded that there are three types of portability: programs, data, and people. Thus, standards relevant to IAP must address the following:

- Source code portability
- Data portability
- User interface
- Documentation portability
- Operating system interfaces
- Communication services
- Database management services
- Software engineering tool interfaces
- Internationalization.

Further, the JTAP study identified the following IAP issues to be addressed in JTC1:

- Standards need to define consistent handling for exceptions encountered by applications during execution.
- Standards need to identify ways to enable adaptation of applications by automated means to accommodate options and other environmental variations (e.g., implementation-defined characteristics, option identification).
- Standards for IAP need to take into account external object names, providing methods to minimize the impact of variations of external object names across application platforms. Language standards need to provide corresponding services and capabilities to enable applications to accommodate these variations (e.g., variable length strings, services for acquiring object names from external sources, object name composition/decomposition).
- Qualitative metrics for application portability may be useful.

IAPs can be language independent, operating system independent, or both. Proposed work in SC21 will be for IAPs that are both language and operating system independent. Language-specific constructs could be developed in SC22, as the mapping of abstract data types to language-specific constructs is primarily the work of defining language bindings.

Specification of an IAP would include definition of data types of the interfaces and may include rules for describing behavior and sequencing of functions within an interface (e.g., blocking or non-blocking procedure calls) and levels of enforcement of these rules. A model of IAPs is needed and should be related to or possibly included in the models for Extended AIX (Application Layer Structure) (XALS) and ODP. It was proposed that the IAP model, as well as the XALS and ODP models, should include a means to extend the interface to include user- or application-specific extensions or abstractions. For example, it should be possible to invoke a procedure to store application data type within the X.500 Directory Service without changing the interface definition. [Ref. SC21 N 4523 1990]

15.1.3.2 Open Systems Environments (OSE)

The IEEE and NIST are promoting the concept of an Open System Environment (OSE), which IEEE P1003.0 defines as:

> *The comprehensive set of interfaces, services, and supporting formats, plus user aspects, for interoperability or for portability of applications, data, or people as specified by information technology standards and profiles.*

An OSE is the basis for profiles. The NIST APP OSE/1 and POSIX are both examples of OSEs. By contrast, a profile, as defined by IEEE P1003.0 is:

> *A set of one or more base standards, and where applicable, the identification of chosen classes, subsets, options, and parameters of those base standards, necessary for accomplishing a particular function.*

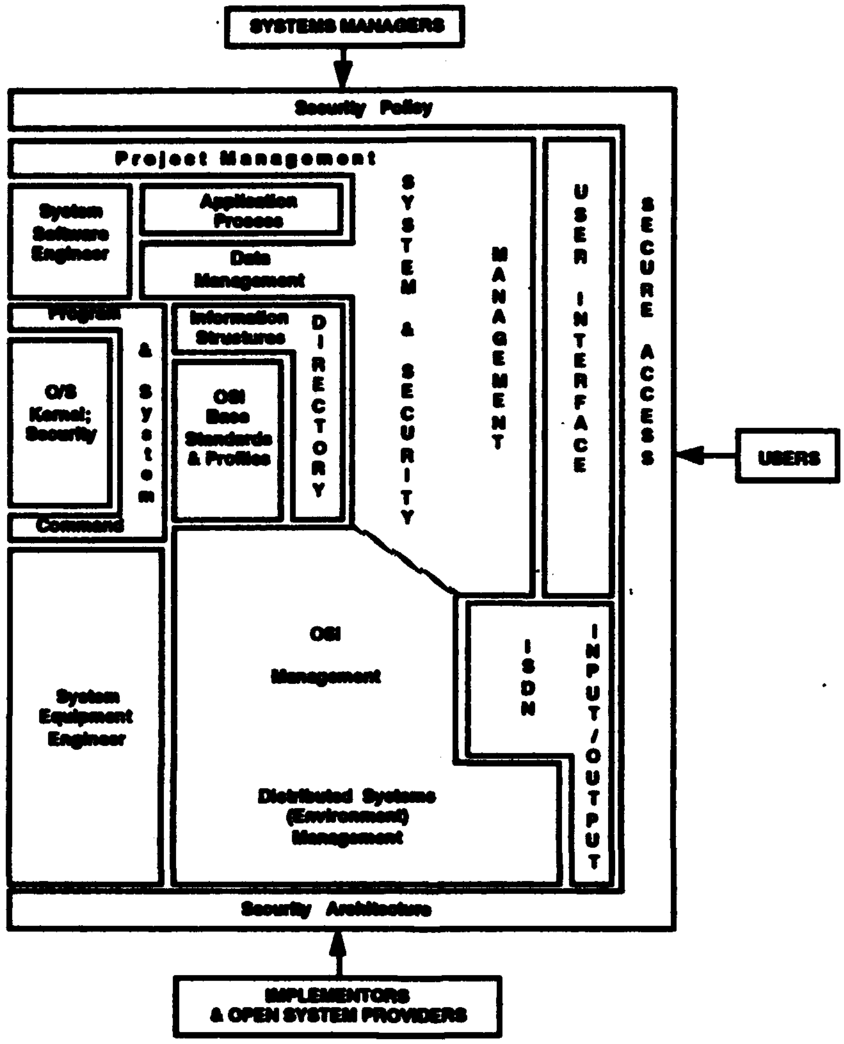
A profile is a list of standards as opposed to an OSE, which is a list of services. Profiles are therefore, subsets of OSEs. They do not specify functionality, but combine multiple base standards, choose and select options and parameters, and address coherence among the base standards. [Ref. Gambrel 1991] Likewise, EWOS has expanded the scope of SGFS to include OSE (see Section 15.1.3.8).

Figure 15 provides an example of a model for an open systems environment developed by the UK MOD [Ref. MOD 1989] and used to promote applications portability. It includes users, developers, managers, and providers. It also explicitly includes security and OSI system and project management.

15.1.3.3 NIST Applications Portability Profile

This section discusses the APP developed by the NIST. The NIST approach to applications portability is based on an architectural approach that provides interfaces for functionality to accommodate a broad range of applications requirements. The functional components of the architecture are viewed as a "tool box" of standard elements that can be used to develop and maintain portable applications. These tools are based on an open systems concept and are required to be developed as an integrated collection of non-proprietary standards. The NIST OSE embraces three concepts:

- <u>Extensibility</u>—Based on an architectural framework that allows an extensible collection of interfaces, services, protocols, and supporting formats to be defined
- <u>Non-proprietary</u>—Interfaces, services, protocols, and supporting formats defined in non-proprietary specifications
- <u>Consensus based</u>—Evolution is controlled by a consensus-based process for definition and specification of interfaces, services, protocols, and supporting formats.



Source: *Scope for MOD Information Technology (IT) Standardization and Responsibilities*, UK MOD Information Technolgy Standards Board, 11 August 1989.
Notes: OS: Operating System
ISDN: Integrated Services Digital Network

Figure 15. A Model for the Open Systems Environment

Moreover, it stresses the following:

- Portability—The ability to use application software and data on heterogeneous hardware and software platforms
- Interoperability—The ability to have application and software operating on heterogeneous hardware and software platforms cooperate in performing some user function
- Scalability—The ability to use the same applications software on many different classes of hardware and software platforms, from personal computers to supercomputers.

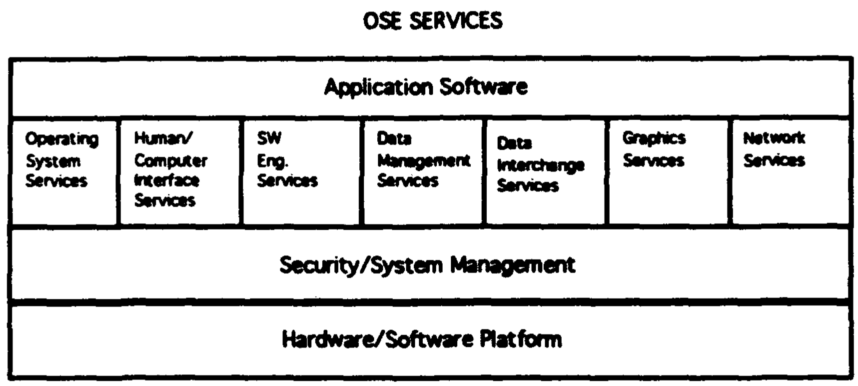
A full complement of standards should be available under the APP by 1995. [Ref. APP 1991] Version 2 of the *Application Portability Profile (APP): The U. S. Government's Open System Environment Profile OSE/1*, NIST SP 500-210 was published in June 1993. It recommends standards and specifications, provides guidance in areas where standards do not exist

for seven service areas, and makes strategic evaluations with respect to those standards. The three strategic classifications are:

- Strategic now—Users reasonably safe in making substantial investment and long-term plans in mission-critical systems and infrastructure
- Strategic in the future—Specifications subject to change but appear to be headed for standardization; some risks but consensus process minimizes them
- Nonstrategic—Stop-gap recommendations with warning that user investment will be at significant risk; not appropriate for long-term planning.

APP specifications are selected according to the following order of precedence: International Standards, US National Standards (e.g., ANSI, IEEE), US National Standards Committee work in progress, other Federal standards (e.g., DoD standards), and specifications that are publicly available and for which implementations are commercially available from a variety of sources (e.g., X-Window System, Version 11). [Ref. Fisher 1991]

Figure 16 provides a high-level view of the architectural approach that underlies the APP.



Source: [Ref. APP 1992]; updated from [Ref. APP 1993].

Figure 16. An Example View of the Architecture for the Applications Portability Profile

Table 38 identifies the elements (tools) and the associated interface specifications of the recommended standards [Ref. APP 1993] for the APP. The key elements are OSI for data communications; (extended) POSIX for the operating system interface; SQL and IRDS for database management; and X-Windows for the human/computer interface.

An extended version of POSIX is recommended in the APP for the operating system interface (see Section 10.2.1). NIST has a FIPS on the Government Network Management Profile (GNMP) for network management (FIPS 179) (see Section 10.2.1.1 and 12.1). SQL (see Section 6.2.2.2) and the Information Resource Dictionary System (IRDS) data dictionary standard [Ref. Goldfine 1988] (see Section 6.2.4) are recommended for database management. The distributed data component will be handled through Remote Database Access (RDA) (see Section 6.2.3). Recommended for data interchange are the following:

- Computer Graphics Metafile (CGM) (see Section 7.2.2.2)
- Initial Graphics Exchange Specification (IGES), used for engineering graphics (see Section 7.2.1.1)
- Standard for the Exchange or Product Model Date (STEP) (identified in Section 7.2.1.2)

- Electronic Manuscript Preparation and Markup (EMPM) (see Section 7.1.2)
- Standard Generalized Markup Language (SGML) (see Section 7.1.2)
- Office Document Architecture/Office Document Interchange Format (ODA/ODIF) (see Section 7.1.1)
- Spatial Data Transfer Specification (SDTS) (see Section 7.3.8).

Table 38. Standards for the Applications Portability Profile

Function	Element	Reference for Standards
Operating System	POSIX	IEEE Std. 1003.1-1990 (FIPS 151-2)
	POSIX SHELL	IEEE Std. 1003.2, September 1992
	REALTIME	IEEE P1003.4
	SECURITY	IEEE P1003.6
Data Management	SQL2	ISO 9075:1992 (FIPS 127-2)
	IRDS	ANSI X3.138-1988 (FIPS 156)
	RDA	ISO 9759:1992
Data Interchange		
- Document interchange	SGML	ISO 8879, ISO 9069, ISO 9070, TR 9573 (FIPS 152)
	ODA/ODIF	ISO 8613
	SPDL	DIS 10180 (planned FIPS)
	EMPM	ANSI Z39.59 - 1988
	EDI	FIPS 161
- Graphic Data Interchange	CGM	ISO 8632 (FIPS 128)
	IGES	NBSIR 88-3813, ANSI Y14.26 (FIPS 177)
- Product Life Cycle Data Interchange	STEP	CD 10303
- Spatial Data Interchange	SDTS	FIPS 173
Graphics Services	GKS	ISO 7942, ISO 8651, ISO 8805 (FIPS 120-1)
	PHIGS	ISO 9592 (FIPS-153)
Network Services		
	GOSIP II	FIPS 146-1
	API	IEEE P1003.12, Draft 2
	ACSE	IEEE P1238
	FTAM	IEEE P1238.1
	GOSIP III	(planned FIPS 146-2)
	ISDN API	Version 1 from ISDN Users Forum
	ISDN	ISDN-FIPS
	OSF DCE RPC	Draft
	TFA	IEEE P1003.8, (planned FIPS)
	GNMP	FIPS 179
	X.400 API	IEEE P1224.1
	X.500 API	IEEE P1224.2
Human Computer Interface	X-Windows	FIPS-158-1
	Modular Toolkit Environment	IEEE P1295.1
Software Engineering Services	C	ANSI X3J11/88-151-Oct 1988, X3.159
	COBOL	ANSI X3.23-1974, 85 (FIPS 021-3)
	FORTRAN	ANSI X3.9-1978 (FIPS 069-1)
	Ada	FIPS 119
	Pascal	ISO 7185-1983 (FIPS 109)
	PCTE	ECMA

Source: *Application Portability Profile—The US Government's Open System Environment Profile OSE/1*, Version 2, NIST Special Publication 500-210, NIST, June 1993.

Graphics Kernel System (GKS) and Programmer's Hierarchical Interactive Graphics System (PHIGS) are recommended for Graphics Services (see Sections 8.2 and 8.3).

Standards and options identified in US GOSIP Version 2 (see Section 16.1.3) are recommended for network services, as well as ISDN and Transparent File Access (TFA). OSF Distributed Computing Environment (DCE) RPC component is recommended for distributed computing services until RPC becomes an international standard. X-Windows is recommended for the human computer interface, providing a non-proprietary windowing capability.

Five standard programming languages are recommended (C, COBOL, FORTRAN, Ada, and Pascal), but standard bindings to POSIX for some of these languages (all but C) are still being defined. [Ref. Martin 1990; Hankinson 1988; APP 1990] In addition, the ECMA's Portable Computer Tools Environment (PCTE) (see Section 4.3.2.2) is being recommended for the programming service environment.

Future updates will be expanded to address distributed computing requirements such as uniformity, transparency, federation, and optimization and to include system security and system management services. Moreover, future updates will include a user requirements framework that will lend a more user-oriented approach to application and organizational profile development. It will consist of a framework and taxonomy for describing user-specified system functionality, examining EWOS and UK work-in-progress as a basis for the user requirements framework.

In November 1993, NIST issued a Draft *Guide on Open System Environment (OSE) Procurements*, which is expected to be published in 1994. The report provides agency program managers, system engineers, and contracting officers with a model for developing the plans and specifications necessary to define the OSE requirements in requests for proposals. Additional information is provided for assisting agencies in determining which portions of the report are applicable to their specific acquisition plans. Lessons learned are highlighted in annotated text that accompanies many of the report's subsections. [Ref. OSE 1993]

The IEEE Computer Society's Portable Application Standards Committee (PASC) [formerly Technical Committee on Operating Systems (TCOS)] has formed a number of working groups to progress POSIX and other standards that are required to facilitate applications portability. Table 39 identifies the documents (and working groups known by the same name) being prepared by IEEE on areas other than POSIX for application portability. [Ref. NIST 1990a] The scope and status of POSIX standards work are discussed in Section 10.2.1.

A review of the interface specifications for the APP shows that there are not yet international standards for many of the elements of the recommended architecture. Some are being considered by ANSI, IEEE, and other standards defining bodies, and others are US standards. For example, X-Windows is being considered by the ANSI X3H3.6 working group, and has been promulgated as FIPS 158. The C language bindings are being considered by the X3J11 ANSI working group. NIST is developing interim standards for file management and is recommending Network File Server (NFS) to IEEE P1003 as the best starting point for these interfaces. [Ref. Hankinson 1988] The engineering graphics standard (IGES) is still only available as a NIST publication.

Table 40 gives an evaluation of the stability and completeness of the standards recommended by NIST for the APP. Each standard in the seven service areas (security is not addressed) is identified by source and given a strategic evaluation: strategic now (STR), strategic in the future (FTR), and non-strategic (GAP).

Table 39. Applications Portability Standards Being Developed by IEEE for Submission to ISO Through ANSI

P1003.0, *A Guide to POSIX Based Open Systems Architectures*—addresses the broad applications portability issues, such as: benefits and risks of open system architecture, architectural framework for portability, applications portability concepts, operating systems services, data management and interchange services, data interchange services, graphics services, network services, user interface services, and languages/application development environment services
P1201.1, *Uniform Application Program Interface*—defines an API for GUI visual objects and windowing services that is implementable on multiple window systems and GUI toolkit APIs. Base document is XVT. Ballot expected 2Q 1993.
P1201.2, *Driveability*—defines a recommended practice for those elements and characteristics of user interfaces that must be consistent to permit users to easily transfer from one look-and-feel or application to another (Ballot June 1992; standard expected mid-1993)
P1201.3, *User Interface Management System (UIMS)*—defines a language-independent dialogue applications programming interface to develop applications systems that are independent of user interface concerns and can be more easily ported across a wide range of user interface styles and technologies; would address such features as: separation of presentation-dependent and presentation-independent aspects, and mechanisms for data and control exchange between application and dialogue layers (not yet approved by TCOS)
1224, *OSI Abstract Data Manipulation API (LIS)*—defines a standard interface supporting the manipulation of complex arguments and parameters used by X.400 and Directory Services APIs, Published 1993.
1224.1, *X.400 Based Electronic Messaging API (LIS)*—defines an X.400 API that makes the functionality of a message transfer system (MTS) accessible to a message store (MS) or user agent (UA)...defines an X.400 Gateway API with two components: a mail system gateway, and an X.400 gateway service. Base document is from X.400 API Association and X/Open. Work to be done before the ballot include. adding language independence features, adding assertions and other test methods, and reformatting the standard into IEEE/ISO form. Published 1993.
1224.2, *Directory Services Application Programming Interface (API)* - Language Independent Specification—defines a language independent API to a directory service including, but not necessarily limited to, ITU-TS X.500 functionality
P1237, *Remote Call Procedure (RPC) Interface Language*—defines an interface description language and a very limited set of procedure interfaces to allow applications to use an underlying RPC mechanism layered on an OSI stack (balloting planned for mid-1992 and approval early in 1993)
P1238 *OSI Application Program Interfaces*—defines an API model for connection-oriented OSI Application Layer services, Draft 14, August 1992. In ballot.
P1238.1, *FTAM OSI Application Program Interfaces*—provides an application program interface to the detailed OSI FTAM services and higher-level user-oriented FTAM-based services (ballot in 1993)
P1295.1, *X Window System Graphical User Interface, Part 1: Modular Toolkit Environment* – defines a source code level interface to an X window system toolkit GUI environment based on OSF MOTIF Application Environment Specification
P1326, *Test Methods for Measuring Conformance to OSI Abstract Data Manipulation - API*—defines the test methods to be used to measure conformance to IEEE Standard 1224
P1326.1, *Test Methods for Measuring Conformance to X.400 Based Electronic Messaging Application Program Interfaces (API) [Language Independent]*—defines the test methods to be used to measure conformance to IEEE Standard 1224.1
1326.2, *Test Methods for* Directory Services Application Programming Interface (API) - Language Independent Specification—defines the test methods to be used to measure conformance to IEEE Standard 1224.2
1327, *OSI Abstract Data Manipulation API*, Published 1993.
1327.1, *X.400 Based Electronic Messaging C Language Interfaces - Binding for Applications Program Interfaces (APIs)*—provides an ISO 9989 C language binding to the language independent API that corresponds exactly with IEEE Standard 1224.1.
1327.2, *Directory Services Application Programming Interface (API) - C Language Specification*—defines a C language API to a directory service including, but not necessarily limited to, ITU-TS X.500 functionality
P1328, *Test Methods for Measuring Conformance to OSI Abstract Data Manipulation C Language Interfaces - Binding for API*—defines the test methods to be used to measure conformance to IEEE Standard 1327

Table 39. (Cont'd)

P1328.1, *Test Methods for Measuring Conformance to X.400 Based Electronic Messaging C Language Interfaces - Binding for Applications Program Interfaces (APIs)*—defines the test methods to be used to measure conformance to IEEE Standard 1327.1
P1328.2, *Test Methods for Directory Services Application Programming Interface (API) - C Language Specification*—defines the general requirements and test methods for measuring conformance to IEEE Standard 1327.2
P1372, *POSIX, Part 1: System Application Program Interface (API) [Language Independent]* is a new POSIX API effort.

Source: "Applications Portability and Open Systems Environments: Status Report," presented by Roger J. Martin, NIST, *10th APP/OSE Workshop*, NIST, Gaithersburg, Maryland, November 1992; updated from IEEE PARs included in a letter from William Rhinehuls, Chairman, SPARC and Convenor, OMC to Kenneth Zemrowski, Chair, X3T5, 1 December 1992 (X3T5/92-478); updated from [Ref. APP 1993].

15.1.3.4 X/Open Common Applications Environment (CAE)

This section discusses the CAE developed by the X/Open international consortium and specified in the X/Open Portability Guide, now in its fourth edition (XPG4). The Portability Guide recommends standards and options within standards to achieve an open environment in which new applications can be ported without modification. Several international consortia have endorsed the X/Open CAE as a basis for developing open environments.

The foundations of the X/Open CAE are the interfaces of the UNIX System V operating system, as defined in the AT&T System V Interface Definition (SVID), and the C language. The X/Open CAE consists of features grouped in seven functional areas: operating system and languages, data management, user interface, general interworking, mainframe interworking, PC interworking, and media.

XPG4, October 1992, addresses the following [Ref. OSN 1992k]:

- X Windows system
- Byte stream file transfer (BSFT) protocol, which refers to ISO 8571 and provides a link between Internet FTP and FTAM
- X.400 electronic messaging specifications
- X.500 directory
- NFS
- IBM's CPI-C communications interface
- PC-NFS server, based on Sun's protocols
- Local Area Network Manager (LMX) for PC interworking, based on Microsoft's LAN Manager for UNIX protocols.

Table 41 shows the XPG4 components and standards for the seven functional areas. Standards, de jure and de facto, where specified, are also shown.

Table 40. Stability of Applications Portability Standards

	STR	FTR	GAP
OPERATING SYSTEM SERVICES			
Portable Operating System Interface for Computer Environments (FIPS PUP 151-2)	●		
NIST Planned FIPS PUB on POSIX Shell and Utility Applications Interface for Computer Operating System Environments (IEEE 1003.2, 1992)			
Amendment 1: Realtime Extension (IEEE P1003.4)		●	
Security Interface for the Portable Operating System Interface for Computer Environments (IEEE P1003.6)		●	
HUMAN/COMPUTER INTERFACE SERVICES			
User Interface Component of Applications Portability Profile (FIPS PUB 158-1)	●		
IEEE P1295.1		●	
SOFTWARE ENGINEERING SERVICES			
Ada (FIPS PUB 119)	●		
C (FIPS PUB 160)	●		
COBOL (FIPS PUB 021-3)	●		
FORTRAN (FIPS PUB 069-1)	●		
Pascal (FIPS PUB 109)	●		
ECMA Portable Common Tools Environment (PCTE)		●	
DATA MANAGEMENT SERVICES			
Information Resource Dictionary System (IRDS) (FIPS PUB 156)	●		
Database Language SQL (FIPS PUB 127-1)	●		
Remote Database Access (RDA)		●	
DATA INTERCHANGE SERVICES			
Office Document Architecture/Office Document Interchange Format (ODA/ODIF), ISO 8613: 1989	●		
Standard Page Description Language (SPDL) (DIS 10180)		●	
Standard Generalized Markup Language (SGML) (FIPS PUB 152)	●		
Electronic Manuscript Preparation and Markup (EMPM) (ANSI/NISO Z39.59-1988)		●	
Computer Graphics Metafile (CGM) (FIPS PUB 128)	●		
Planned FIPS Initial Graphic Exchange Specification (IGES)	●		
Standard for the Exchange of Product Model Data (STEP), ISO CD 10303		●	
Electronic Data Interchange (EDI) (FIPS 161)	●		
Spatial Data Transfer Specification (SDTP) (FIPS 173)	●		
GRAPHICS SERVICES			
Graphical Kernel System (GKS) (FIPS PUB 120-1)	●		
Programmer's Hierarchical Interactive Graphics System (PHIGS) (FIPS PUB 153)	●		
NETWORK SERVICES			
IEEE P1003.12 Protocol-independent Interfaces (PII)		●	
IEEE P1238 OSI API		●	
IEEE P1238.1 File Transfer Access and Management (FTAM) API		●	
GOSIP Version 2 (FIPS 146-1)	●		
ISDN API		●	
ISDN Protocols		●	
OSF DCE Remote Procedure Call			●
IEEE P1003.8 Transparent File Access		●	
Government Network Management Profile (GNMP) (FIPS 179)	●		
IEEE P1224.1 X.400 Electronic Messaging API		●	
IEEE P1224.2 X.500 Directory Services API		●	

Sources:
Application Portability Profile -- The US Government's Open System Environment Profile OSE/1, Version 2.0, NIST, US Department of Commerce, May 1993, UNCLASSIFIED.

Key:
STR Strategic now (relatively stable).
FTR Strategic in the future (subject to change but nearing standardization).
GAP Nonstrategic (stop-gap measure, not appropriate for long term planning).

Table 41. XPG4 Components and Standards

Subject Area	Components	Standards
Operating System and Languages	Internationalized System Calls and Libraries	ISO 9945-1:1990 (POSIX.1)
	Commands and Utilities	ISO 9945-2:1992 (POSIX.2)
	C Language	ISO 9899:1990
	COBOL	ISO 1989:1985, 1989/AM1
	Pascal	ISO 7185:1983
	FORTRAN	ISO 1539:1980
	Ada	ISO 8652:1977
Data Management	ISAM	*De facto* industry standard C-ISAM by Informix Corporation
	Relational Database	ISO 9075:1992 (SQL)
User Interface	X-Window System Display	
	X-Window Services to Applications	
	Terminal Interfaces	
General Interworking	BSFT	ISP 10607, ISO 8571
	X.400 Gateway	ITU-TS X.400
	X.400 Message Access	ITU-TS X.400
	Directory Access	ISO 9594 (ITU-TS X.500)
	Network File System	
	Transport Service	X/Open Transport Interface (XTI)
Mainframe Interworking	CPI-C	IBM CPI-C, Version 1
PC Interworking	PC (NFS Server)	
	LMX Server	
Media	Magnetic Media	

XPG4 provides components that can be separately branded or collected together to match a profile. An XPG4 Component is the smallest unit that can be branded. The Internationalized Systems Calls and Headers within the Operating System and Programming Language subject area broadly corresponds to ISO 9945-1:1990 (POSIX.1). However, the ISO standard defines only a subset of the operating system interfaces required by applications developers and also allows for some optionality and alternative behavior. The X/Open System Interfaces remain that of a complete operating environment and contain many additional interfaces and features. To satisfy internationalization requirements, X/Open Systems provide full data transparency to applications, allowing flexibility in the choice of coded character set(s). In addition, the system must allow program messages to be handled in the native language of the user, as well as provide culture-dependent data items. Internationalization activity has been concentrating on the support of Eastern languages and cultural differences, and of multi-byte code sets in general.

Data management includes Indexed Sequential Access Method (ISAM) interfaces that are defined for creating, managing, and manipulating indexed files, and SQL for access to relational database management systems. The ISAM definition is based on Version 2.10 of C-ISAM by the Informix Corporation. SQL is based on ISO 9075:1992 but contains extensions and deviations (see Section 6.2.2.2).

User Interface work within the X/Open environment covers X/Open Window Management Specifications for the X Window System Protocol, X Toolkit Intrinsics, and Inter-client Communications Conventions Manual. The Xlib interface has been brought up to the X Window System 4 release level.

One of X/Open's major objectives is to facilitate effective interworking between X/Open-compliant systems. The XPG4 Transport Service is an update to the XPG3 component, with

modifications and extensions, particularly in the area of option management, and in the addition of support for NetBIOS.

In the area of PC interworking, XPG3 provided support for the use of workstations and personal computers as terminals connected to open systems using asynchronous serial links with terminal emulation and file transfer. X/Open has replaced these facilities to provide for file access and print services. The XPG4 (PC) NFS component defines the NFS protocols that must be supported by an X/Open-compliant system in order to act as a file and print server to a network of DOS-based personal computers. The XPG4 LMX server component defines the LMX protocols that must be supported by an X/Open-compliant system in order to act as a file and print server to a network of DOS-based personal computers.

One of the major problems inhibiting the porting of applications between X/Open Systems is that of incompatible media and the physical problems of transferring source code in machine-readable form. Common specifications were defined in XPG3 as "Source Code Transfer." The media definitions in the Source Code Transfer component of XPG3 have been updated. The physical size/shape and the recording format are described. Provisions for 1600 bpi and 6250 bpi magnetic rapes are carried forward, but 5.25-inch and 3.5-inch 720-Kbyte floppy discs are no longer mandated. [Ref. X/Open 1992]

15.1.3.5 Open Software Foundation (OSF) Profiles

OSF has announced an API specification called the Application Environment Specification (AES). The RPC AES was printed by Prentice Hall in October 1993. The time service AES material has been reviewed by X/Open, with the directory service currently undergoing X/Open and OSF member review. Security and threads AES sections are making good progress; OSF expects to have these sent to X/Open for review by the end of 1993. Distributed File System (DFS) AES material will be developed in 1994. X/Open will include these in XPG specifications. These AES sections will complete Revision A of the AES, which corresponds to 1.0.X. OSF will update these with 1.1 features to produce Revision B when 1.1 products are in the marketplace.

Revision 1.1 is to be expected to be available in the third quarter of 1994. It will have extensions in the area of security, internationalization, and serviceability as well as better interoperability with Microsoft RPC clients.

OSF is managing a group on behalf of X/Open to specify an extensible architecture for integrating name directory servers. This project is known as the Federated Naming project. It includes technical participation from OSF, HP, Sunsoft, SNI, IBM and Banyan, and one or two additional participants are expected before the project is completed. The output of this project will be an API specifying a programming interface suitable for use with directory servers that are used to compose a namespace at runtime, along with a protocol that can be exported by directories that wish to participate in the namespace. (It may be considered a backplane for directory integration.) It does not increase interoperability of directories, although it provides a methodology for others to accomplish this. As part of this project, the participants will prototype this API over a variety of existing directory services, including CDS, NIS+, and X.500. OSF expects to incorporate this API in a future version of DCE (see Section 13.4.1) to allow additional directory servers to participate in the DCE global name space. X/Open will publish and revise the resulting specification. The group has a draft API specification suitable for beginning the prototyping effort. The prototype effort will require a few months to develop and assess, with resulting changes to the specification incorporated at its conclusion.

The Open Systems Foundation Research Institute is also working on an architecture-neutral distribution format (ANDF). This project promises to produce a methodology that can assure application portability without requiring access to source code. The specification and technology will permit compilation of the source to an intermediate form that is distributed to users. The user will install the intermediate form by compiling it to final form for each platform. Assuming that a platform is replaced by another, the intermediate form could be recompiled for the new platform. ANDF use assumes the existence of an "installer" for the platform to be used; it also assumes that a standardized library and set of APIs exist on each platform.

The base technology for ANDF comes from the United Kingdom's Defense Research Agency (DRA). DRA plans to commercialize this technology. An experimental, non-commercial release is expected by the first quarter of 1994. Commercial release is expected in the second quarter of 1994. ESPIRIT projects in 1995 should produce additional products.

15.1.3.6 Technical and Office Protocol (TOP)

The TOP is part of a combined industrial and government effort on the part of users in the office and engineering community to specify a profile of standard protocols that can be used in commercial applications to provide connectivity and interoperability. TOP is associated with another effort, Manufacturing Automation Profile (MAP) (see Section 9.11.5.1).

The TOP specification [Ref. Thacker 1987] defines a functional network for distributed information processing for technical and business functions. TOP Version 1.0 (November 1985) provides for Carrier Sense Multiple Access/Collision Detection (CSMA/CD) and Token Bus LANs using the connectionless or X.25 Internet Protocol and the Class 4 transport protocol, with FTAM supported at Layer 7.

TOP Version 3.0 was released in 1989, and it is expected to have a six-year stability period before release of another version. It provides not only FTAM but also VT, Directory services, network management, and MHS at Layer 7. It further includes the ODIF (ISO 8613), Computer Graphics Metafile (CGM) Interchange Format (ISO 8632), Product Definition Interchange Format (PDIF), and the GKS interface (ISO 7492). IGES Version 3.0 from ANSI [Ref. ANSI Y14.26M-1986, IGES 1986] is included. At the lower layers, TOP Version 3.0 provides for Token Ring LANs and for X.25 packet switching via X.21 and X.21 bus at Layer 1. TOP Version 3.0 is summarized in Table 42. Future editions of TOP are expected to point to IGOSS (see Section 16.1.3.3).

The international organization, Open Systems Interconnection for Technical and Office Protocol (OSITOP), has been examining architectural issues and has produced a position paper on a solution for connection-oriented network service (CONS) and connectionless-oriented network service (CLNS) internetworking (see Section 9.12). This paper reaches the following conclusions:

- It is not realistic to sidestep the CONS vs. CLNS issue by expecting that one of the two incompatible sets of protocols (CONS or CLNS) be abandoned or by accepting the existence of two non-communicating OSI islands.
- Three solutions are valid, although not architecturally correct according to OSI principles:
    - The "265" internetworking function (based on TP4 over CONS)
    - A Distributed System Gateway (DSG)
    - A Multi-System Distributed System Gateway (MSDSG).
- OSITOP recommends the MSDSG solution.

Table 42. Standards for TOP Version 3.0

Layer	References for Standards
7. Application	ISO 8571 (FTAM) ITU-TS X.400-1984 (MHS) ISO 9041 (VT, subset VT-B) ISO 8613 (ODIF) ISO 8632 (CGM) ISO 7492 (GKS) ISO 9594 (Directory) ISO 9595 and 9596 (Network Management) ISO 8649 and 8650 (ACSE)
6. Presentation	ISO 8823
5. Session	ISO 8327
4. Transport	ISO 8073 (Transport Class 4)
3. Network	ISO 8473 (CLNP, SNDCP) ITU-TS X.25 PLP
2. Data Link	ISO 8802/2 (Type 1, Class 1 Logical Link Control) ITU-TS X.25 HDLC (LAPB)
1. Physical	ISO 8802.3 (CSMA/CD) ISO 8802.4 (Token Bus) ISO 8802.5 (Token Ring) ITU-TS X.21 and X.21 bus (Packet Switching)

PLP: Packet Level Protocol
HDLC (LAPD): High Level Data Link Control (Link Access Procedure Version D)

15.1.3.7 Multivendor Integration Architecture (MIA)

Nippon Telegraph and Telephone Corporation (NTT) has announced the introduction of its Multivendor Integration Architecture (MIA). The architecture, developed together with NTT Data Communications Systems (NTT DATA) and five computer vendors (IBM Japan, Digital Japan, NEC, Hitachi, and Fujitsu), will enable the creation of systems composed of different vendors' computers. The architecture has been developed with the intention of providing a multivendor system that users will find easy to use. The information processing system software consists of an operating system with user programs, databases, and interface programs installed for connecting terminals and other equipment. In developing MIA, preference was given to international standards such as program language specifications and communication protocols that have been time-tested. In areas that have not yet been standardized, the emphasis was on determining what would be necessary from the user's standpoint. In adopting the specification, efforts were focused on either expanding the international standards or on adopting de facto standards and specifications proposed through joint research. MIA consists primarily of three interfaces common to vendors [Ref. OSN 1991a]:

- Application Program Interface (API). The interface located between basic software and application programs that sets the specifications for three programming languages (COBOL, FORTRAN, and C) and the database language SQL, based on ISO and ANSI standards. An interface called the *Structured Transaction Definition Language (STDL)* was newly specified for the communication access interface and user access interface for distributed transaction processing.
- System Interconnection Interface (SII). This prescribes a communication protocol consisting of four types of upper-layer protocol specifications: file transfer, mail transfer, distributed transaction processing, and network management. The lower layer protocol specifications are also prescribed based on Internet and OSI.

- Human Interface (HUI). MIA uses three types of human interface specifications from OSF/Motif, OPEN LOOK, and IBM's Common User Access (CUA).[75] These three interfaces, which are becoming industry standards, are used with UNIX and IBM's OS/2.

15.1.3.8 EWOS Profiles for the Open System Environment (OSE)

EWOS has been studying the application of profiling concepts to the domain of OSE since it proposed (ENV 40002) to create European functional standards for the CAE (see Section 15.1.3.4). ENV 40002 applies the methodology for OSI profiles to the CAE domain, so that the use of the corresponding base standards could also be specified in a similar way for use in procurement.

EWOS has issued a draft document on OSE profiles (EWOS/TA/91/68, April 1991). The document covers the use of standards in a number of broad domains:

- User access techniques
- POSIX interfaces (ISO 9945)
- APIs to system and information services
- Data formats for storage and interchange
- OSI protocol profiles
- Application development tools, languages, and bindings
- Internationalization.

If approved, it would be forwarded to ISO's SGFS for functional standardization. Table 43 shows the proposed taxonomy for OSE profiles.

15.1.3.9 UNIX International's ATLAS (UI-ATLAS)

UNIX International recently announced its UI-ATLAS Distributed Computing Program that has the support of 20 companies. UI-ATLAS is designed to meet five challenges to the open systems industry [Ref. UNIX 1991]:

- Provide a framework for systems software beyond the operating system level that delivers a complete open systems environment.
- Provide a model for allowing alternative technologies through standard interfaces (APIs, protocols, and data formats) without loss of investment.
- Interoperability with the installed base of computer systems to protect customer investments.
- Harmonize the industry's diverse approach to open systems technology by allowing the implementation of competitive technologies under a single framework.
- Provide a new paradigm for distributed applications that uses object orientation to better manage the complexities inherent in heterogeneous distributed computing.

15.1.3.10 Desktop Management Interface (DMI)

DMTF's (see Section 15.1.2.6) DMI is a set of APIs for managing desktop systems. The DMI architecture was announced in August 1992 and the specifications are expected to be released as a reference document later in 1993. Beta code was shipped to group members in May 1993, including test implementations of the interface, and managed objects for hardware, software, and add-in components. Compatibility issues have been considered and the group will produce application software that tests compliance. So far the work has focused on IBM-compatible PCs,

---

[75] CUA is the user interface portion of IBM's Systems Application Architecture (SAA).

but the architecture can be ported and DMTF encourages future support for the Macintosh and UNIX. The final reference kit will include the API definitions, a local test application, and Windows and DOS versions of the service layer code. Reference documents and code will be available free of charge from any of the eight DMTF founders. DMTF expects a market in DMI-compliant products to develop in the next 2 years. IBM is investigating incorporating it into the AIX, OS/2, and DOS operating systems. Microsoft plans to incorporate DMI into DOS, Windows, and NT. Intel will include DMI compliance in the next version of its LAN adapters, and management products. [Ref. OSN 1993g]

Table 43. EWOS Profiles for the Open System Environment

POEnn	Open System Environment Profiles		
	POE0	Base Environment	
	POE1	Workstation Environments	
		POE10	Terminal Environment
		POE11	Personal Workstation Environment
		POE12	Professional Workstation Environment
	POE2	Utility Server Environments	
		POE20	Electronic Message Serving Environment
		POE21	Directory Serving Environment
		POE22	Access Control Serving Environment
	POE3	Information Server Environments	
		POE30	DBMS Server Environment
		POE31	Document Serving Environment
	POE4	Transaction Processing (TP) Environments	
		POE40	Simple TP Environment
		POE41	Enhance TP Environment
	POE5	Real-time Environments	
		POE50	Real-time Environment, seconds
		POE51	Real-time Environment, milliseconds
	POE6	Supercomputing Environments	
POCaa	Open System Environment Components		
	POCA	Application Program Interfaces	
		POCAM	APIs for Management Services (e.g., APIs to access and manipulate managed objects)
		POCAU	APIs for End-User Services (e.g., FIMS API)
		POCAS	APIs for System Services (e.g., ISO 9945-2)
		POCAI	APIs for Information Services (e.g., ISO 9075.2)
		POCAC	APIs for Communication Services (e.g., X.400 API)
	POCL	Look-and-Feel Definitions	
	POCF	Formats	
	POCP	Protocols	

POC: Profiles for Open System Environment Components
POE: Profiles for Open System Environments

15.1.3.11 Service Providers Integrated Requirements for Information Technology (SPIRIT) Project

The SPIRIT Project [OSN 1993t] is developing a telecommunications service providers' (Telcos) procurement specification for a general purpose computing platform. The project, which started in mid-March 1993, includes AT&T, Bellcore, BT, ETIS, France Telecom, KDD, NTT, STET and Telefonica. It aims to define a common specification and has released the first version. The project will run for 2 years, and the work will proceed in three phases:

- Phase A compared the existing documents of the service providers, to derive a statement of common components.
- Phase B will progress phase A selections and select emerging technologies
- Phase C will concentrated on producing requirements for newer technologies.

15.2 Applications Programming Interfaces (APIs)

APIs define the interface to communications and other services.[76] Programs that use them will be more portable, able to work with other services, and run in other environments. APIs serve to decrease the need for platform-specific application programming. Although APIs are outside the original scope of the OSI standardization scheme, many groups are defining APIs for various communications services within the OSI program. A November 1993 *Information Week* article [Ref. Stahl 1993] characterizes APIs as one type of *middleware*, go-between software that is crucial to distributed computing (see Section 13.5).

Vendor-Independent APIs. Figure 17 shows a vendor-independent set of APIs for the OSI environment. Some of the vendor-independent APIs defined by several consortia or groups for the OSI environment include:

- Manufacturing Automation Protocol (MAP) 3.0
  - *Connection Management Interface Specification (CM-IS)*
  - *Private Communication Application Interface Specification*
  - FTAM API
  - MMS API (see Section 9.11.5.1)
- UNIX International
  - *ACSE/Presentation Layer Interface (API)*
  - *Transport Layer Interface (TLI)* and the *Transport Layer Protocol Interface (TPI)*
  - *Network Layer Interface (NLI)* and *Network Protocol Interface (NPI)*
  - *Data Link Protocol Interface (DLPI)*
- X.400 Applications Programming Interface Association (XAPIA and X/Open)
  - *X.400 API Specification (X.400)*
  - *X.400 Gateway Specification*
  - *OSI Object Management API (XOM)*
- X/Open
  - *X/Open Transport Interface API (XTI)*
  - *X/Open ACSE/Presentation Service API (XAP)*
  - *X/Open Common Programming Interface-Communications (CPI-C)*
  - *X/Open Directory Services API (XDS)*
  - *X/Open FTAM API (XFTAM)*
- IEEE
  - P1003.8, *Transparent File Access*
  - P1003.12, *Protocol-Independent Interfaces*
  - P1003.17, *Namespace and Directory Services*
  - P1224, *API to Management Functions for ASN.1 Objects*
  - P1224.1, *API to ITU-TS X.400 User Agent and Message Transfer Agent*
  - P1224.2, *Directory Services Application Programming Interface (API) - Language Independent Specification*

---

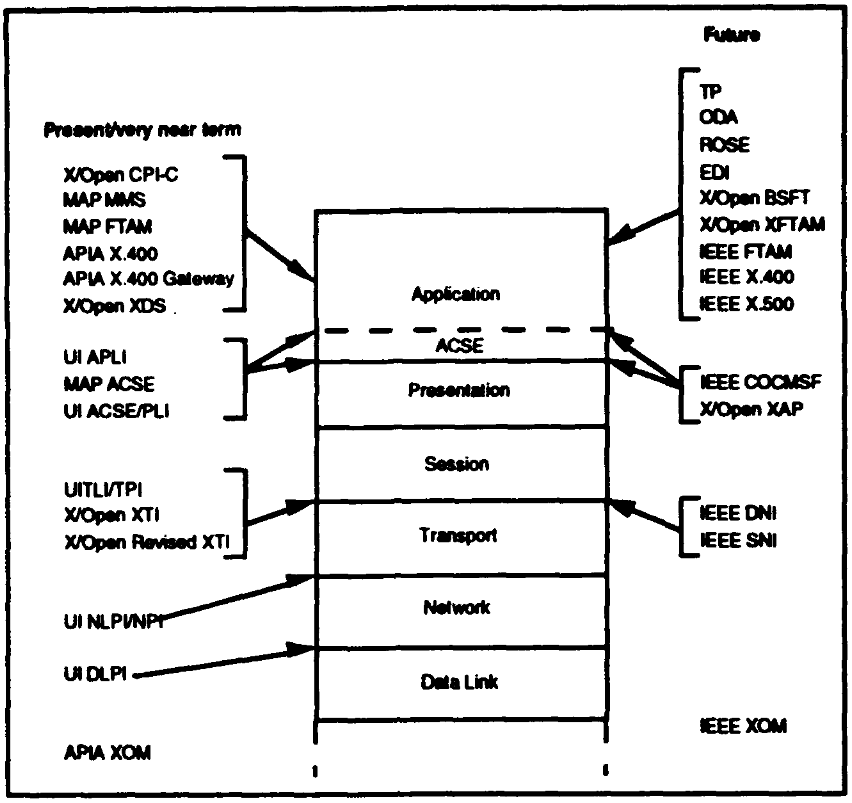
[76] Discussion taken from "A Users' Guide to Data Communications APIs," by Eric Fleishman, *OSN: The Open Systems Newsletter*, vol. 6, nos. 5 and 6, June and July 1992 issues.

- P1238, *API to Common OSI Connection Management and Support Functions*
- P1238.1, *API to FTAM*
- P1326, *Test Methods for Measuring Conformance to OSI Abstract Data Manipulation - API*
- P1326.1, *Test Methods for Measuring Conformance to X.400 Based Electronic Messaging Application Program Interfaces (API) [Language Independent]*
- P1326.2, *Test Methods for Directory Services Application Programming Interface (API) - Language Independent Specification*
- P1327, *OSI Abstract Data Manipulation API*
- P1327.1, *X.400 Based Electronic Messaging C Language Interfaces - Binding for Applications Program Interfaces (APIs)*
- P1327.2, *Directory Services Application Programming Interface (API) - C Language Specification*
- P1328, *Test Methods for Measuring Conformance to OSI Abstract Data Manipulation C Language Interfaces - Binding for API*
- P1328.1, *Test Methods for Measuring Conformance to X.400 Based Electronic Messaging C Language Interfaces - Binding for Applications Program Interfaces (APIs)*
- P1328.2, *Test Methods for Directory Services Application Programming Interface (API) - C Language Specification.*

P1003.12 will provide a portable interface to both high-level and low-level transport services. The high-level interface is referred to as the Simple Network Interface (SNI); the low-level interface will be based on Berkeley Sockets and the X/Open XTI. P1238 provides a high-level interface to ISO upper layer services. It will permit developers of OSI application services such as message handling, FTAM, Directory, and network management to use a common upper layer platform and focus development efforts on the application services themselves. [Ref. IGOSS 1993]

Data Management APIs. Several data management initiatives will define APIs (see Section 6.2.2.2). ANSI is working on SQL3 as a future API for conforming database management systems (usually relational). The SQL Access Group and X/Open are working on an API and SQL-standard for client-server interactions. Microsoft has produced an Open Database Connectivity (ODBC) standard, which is based on early work of the SQL Access Group and X/Open. Brained, Novell, IBM, and others are working on the Integrated Database Application Programming Interface (IDAPI). [Ref. RNLA 1994, p. 31]

Messaging APIs. In the past, there has been considerable confusion over which electronic mail API users and developers should support. Recently, however, Novell Inc.'s Message Handling Service (MHS) API has eclipsed competing APIs including Lotus Development Corporation's Vendor Independent Mail (VIM) and Microsoft Corp.'s Mail Application Programmer Interface (MAPI) and has emerged as the most popular mechanism. The commercial vendor community is standardizing on the Common Mail Calls (CMC) specification developed by X.400 Application Programming Interface Association (XAPIA). While the alignment of MAPI and VIM forces is good news for users, questions remain about the technology on which extensions to CMC will be based and whether key vendors will continue to support the new interface extensions. [Ref. Rash 1993]



Source: "A Users' Guide to Data Communications APIs," Pt. 2, by Eric Fleishman, *OSN: The Open Systems Newsletter*, Vol. 6, No. 6, June 1992, p. 2.

Key:
ACSE — Association Control Service Element
APIA — X.400 Applications Programming Interface Association
APLI — ACSE/Presentation Layer Interface
BSFT — Byte Stream File Transfer
COCMSF — Common OSI Connection Management and Support Functions
CPI-C — Common Programming Interface - Communications
DLPI — Data Link Protocol Interface
DNI — Detailed Network Interface
FTAM — File Transfer, Access and Management
MAP — Manufacturing Automation Protocol
MMS — Manufacturing Message Specification
NLPI — Network Layer Protocol Interface
NPI — Network Protocol Interface
PLI — Presentation Library Interface
SNI — Simple Network Interface
TLI — Transport Layer Interface
TPI — Transport Layer Protocol Interface
UI — Unix International
XAP — X/Open ACSE/Presentation API
XDS — X/Open Directory Services
XOM — OSI Object Management API
XTI — X/Open Transport Interface

Figure 17. Vendor-Independent APIs for the OSI Environment

Long-Term API Standardization. In June 1992, JTC1/SC21 initiated a study period on the international standardization of APIs and raised the following short- and long-term considerations. In the short term, SC21 notes that there has been significant international activity

and agreement on the development of three particular APIs: (1) the MHS API, (2) the OSI Directory API, and (3) the OSI Abstract-Data-Manipulation API. Work on these APIs has been progressed in the X.400 API Association, X/OPEN, and IEEE since 1988 and is mature and widely known. Implementations exist based on these specifications, and SC21 considers that this work should be progressed expeditiously within JTC1 and anticipates that no major modifications will be needed.

The first meeting of the SC21 study group on APIs was held in Boulder, Colorado, in November 1992. There was strong agreement among the participants on the importance of this subject for international standardization and the value of the Reference Model of Open Distributed Processing (ODP-RM) to guide the work. Moreover, it was agree that the term *application* programmatic interface (API) is misleading because one person's application is another person's infrastructure. It was agreed that a programmatic interface that is subject to international standardization should be called a standard programmatic interface (SPI). The urgency of the public's need for standard programmatic interfaces led the group to propose that SC21 shorten the study period to one year and take action at the Yokohama meeting. The output of the meeting was SC21 N 7425, *Draft First Report on the New Work Area on Programmatic Interfaces*, November 1992. [Ref. SC21 N 7424 1992]

In June 1993 at its Plenary, SC21 approved SC21 N 8045 Revised, *The Report of Programmatic Interfaces*, as the SWG-API final report. This report concluded that there was a strong requirement for standardization of programming interfaces and a need for a framework in which the work could be carried out. During the June 1993 plenary, SC21 dissolved the SWG-API, and agreed to establish a Special Working Group on the Standardization of Programming Interfaces (SWG-SPI). The output of the November 1993 meeting of the SWG-SPI addressed an architectural framework, technical guidelines, and conformance methodology. [Ref. SC21 N 8397 1993]

In a liaison statement of December 1993, the SGFS provided the following notes on the further investigation of APIs in relation to profiles [SGFS N 1087 1993]:

- The SGFS intends to define (or provide provisions for) profiles that combine APIs and protocols into some higher level of profiles.
- An API does not directly use another API. The functionality offered through an API may *use* another API, but this need not lead to a fixed relationship between APIs.
- Profiling systems in such a way that one functionality invokes another through an API puts constraints on the implementation. This is an issue when exchanging components of a profile, but it is not relevant for application portability and interoperability.

In September 1993, the OIW raised the following concerns regarding TR 10000-3 and distinguishing between application portability and system software portability [Ref. SGFS N 1065 1993]:

- Changing the objectives to allow system software portability (application platform decomposition) fundamentally conflicts with other current objectives (implementation transparency and accommodation of new technology).
- Such a change in objectives is out of scope with and conflicts with the agreed definition of Open System Environment (*The Way Ahead* [SGFS N 402]).

- System software portability issues, constituencies, and standards are very different from those related to application portability.
- It is important that ongoing work addressing the users' need for application portability not be delayed while issues surrounding system software portability are resolved.

The OIW further noted that the EWOS and the OIW agree that the world needs to understand how software such as COBRA, DCE, TP, and databases fit together. These enabling technologies are considered as middleware—the users do not see them but they give the capability to accomplish user tasks. The OIW proposes a model to reflect how middleware is to be incorporated, using the model of the IEEE P1003.0 draft guide as a basis. Completion of the model should not disturb the existing OSE consensus on methods for achieving applications portability and would be the basis for developing new concepts for application software decomposition.

In December 1993, the SGFS developed a *White Paper on OSE Profiling Concepts* [Ref. SGFS N 1089 1993] that discusses the issues of application portability and interoperability and addressed the longer-term need (expressed by some national bodies) for a level of exchangeability of software components. This paper is designed, in part, to be consistent with the user-oriented view contained in the *Software Integration Platform Specification* provided by the Petrochemical Open Software Corporation [SGFS N 1070]. The paper notes an agreement that a major purpose of OSE profiling (TR 10000-3) is the preparation of application platform (AP) profiles that specify the behavior of APs to meet user requirements. The AP is viewed as a black box and the corresponding AP profile specifies its behavior in terms of the behavior that can be observed at its interfaces and the relationship among the behaviors at different interfaces. AP profiles for an AP entity comprise HCIs (interactions with human beings), information interfaces (to information service entities), and communications interfaces (to communication service entities). Example elements of AP profile specifications would include Motif, style guides, and XHRS Windows for HCI; SQL, RDA, XTI, and mOSI for database interfaces; XTI and TA 51 for lower layer communications interfaces; and POSIX for operating system interfaces. Exchangeability is modelled as a property of a software element such that it can be placed outside the AP and that interfaces between it and the AP can be defined in implementation terms (e.g., as APIs).

In a January 1994 report to JTC1, the Chair of SC21 noted a two-pronged approach recommended by the SC21 Study Group on APIs:

- Short-term work to: (1) identify candidate specifications for programming interface standardization related to standards for which SC21 is responsible; (2) request use of new work item proposals and fast-track procedures to progress these specifications; and (3) request submitters to identify the SC(s) responsible for the underlying function and the programming language(s), state whether the programming interface specification require extensions to a programming language or service, characterize the expertise required to develop the specification, and identify relationships of the specification work to other work of the various SC(s) involved.
- Long-term work, using a Joint Working Group on Programming Interfaces administered either by SC21 or SC22, to produce a standard covering architectural framework, technical guidelines, and conformance methodology.

The basis for the January 1994 report to JTC1 was the June 1993 Report of the SC21 Study Group on APIs [SC21 N 8045 Revised]. The Study Group met in November 1992 and June 1993. The report emphasized the central role of effective and well-coordinated standards for programming interfaces to the growth of open distributed systems. Without such standardization, integration of open systems components on each vendor platform will be more difficult and

expensive; business application software will be developed using ad hoc proprietary interfaces with resultant increase in costs to integrate that software into an enterprise's systems; development of standard applications will be hindered; distributed applications will be less portable; and skills of applications programmers will be limited to specific platforms. [Ref. SC21 N 8045 Revised 1993]

The report emphasized programming interface—an interface between one software component and its supporting infrastructure—over API because the term "application" has sometimes been interpreted simplistically to mean an interface between a business application, such as an order processing system, and an operating system, such as is described by POSIX and because the applications elements for an infrastructure may become the infrastructure for other elements. When a programming interface has become a standard, the term standardized programming interface (SPI) would be used. The following paragraphs highlight some of the concepts expressed in the Study Group report. [Ref. SC21 N 8045 Revised 1993]

Requirements for Interface Specifications. An interface specification specifies the interactions of functional components of systems. It identifies the operations that can be performed at an interface, the state of the communicating objects affected by the operations, and the circumstances in which the operations are appropriate. In addition, a specification may be structured (e.g., using the concept of viewpoint) to reflect a number of different design concerns relating to specific behavior, consistency, or enterprise policy. High-level descriptions are refined into distinct, specific descriptions of the detail of programmatic, interworking, or other forms of interactions. Thus, an interface specification will consist of two parts: (1) the specification of the behavior observable at the interface and (2) the specification of the context within which the function being accessed operates. [Ref. SC21 N 8045 Revised 1993]

Programming Interface Specification Framework. A framework is needed to identify and position interfaces relative to one another and to describe what combinations of interfaces are possible and meaningful. The framework is based on a set of technical concepts necessary to ensure consistency across definitions of interface, interaction, state, and behavior. Standardized interfaces for different kinds of reference points, such as programmatic, interworking, perceptual, and interchange reference points and enable precise specification of relationships that may exist between them. [Ref. SC21 N 8045 Revised 1993]

Such a framework needs to express a range of API concepts. APIs may conceal much of the detailed capabilities of a function or may allow them all to be controlled directly. Some APIs may be independent of which services support them and may allow service selection to be based on factors expressed in such user-oriented terms as urgency, security, cost, or service availability. Other APIs may be specific to a particular function. The framework needs to address whether there should be a limit on scope of the functions an interface may describe—a function may be described either as a traditional programming interface or as an object providing a service. [Ref. SC21 N 8320 1993]

From the OSI perspective, an API defines a real interface, invocable by a real process, to a collection of related services provided by one or more finite state machines that implement one or more OSI (though not necessarily standardized) services. A framework needs to identify the relationships of these APIs to the underlying service services and structure of the APIs that may be derived from the architecture relating these underlying services. For OSI, a real open-system may have any number of APIs, all of which are directly or indirectly defining concrete, language-oriented access methods to abstract services defined by (1) one or more standardized OSI service

definitions, (2) one or more non-standardized OSI service definitions, and (3) modifications from control functions as defined in ISO/IEC 9545. Where an abstract service is to have APIs for more than one programming language, there should also be a language-independent specification of the API to ensure semantic consistency of the several language-dependent APIs. A language-independent API specification indirectly defines the language-dependent access method to the underlying abstract service. [Ref. SC21 N 8316 1993]

Potential Use of the ODP Reference Model (RM-ODP) for Interface Specification. The RM-ODP defines the interface concept, interaction, interaction point, behavior, and state. The five RM-ODP viewpoints (enterprise, information, computational, engineering, and technology) can be used to identify and separate general concerns that may intervene in the specification of an interface. The Viewpoint Languages of RM-ODP potentially provide a single interface specification technique. For example, the ODP Computational Language provides the means to define interface types and behavior in a manner independent of actual localization of interfaces and of programming languages. Further, the Engineering Language provides a general structure wherein several interfaces are identified and defined and services may be specified. In addition, RM-ODP provides a general conformance framework that identifies the different types of reference points that may coexist in an open distributed system and discusses the conditions under which testing a system that claims conformance to several different interface specification standards can be done. Finally, the Architectural Semantics of the RM-ODP provides an interpretation of the basic concepts associated with the notion of interface using existing formal description techniques standardized by SC21.

Relation to IDNs. Several activities are being carried out in JTC1 that can eventually lead to standard programming interfaces (SPIs). These include Common Language Independent Data Types (ISO/IEC 11404), Common Language Independent Procedure Calling Mechanisms (SC22 N 1082), and RPC Interface Definition Notation (IDN; DIS 11578-2). When mappings from IDN to programming languages become available, interfaces defined using IDNs can also be expressed in the form of a derived SPI specification with language bindings.

15.3 Conformity to an Open System Environment

JTC1 has established a Special Working Group on Conformity Assessment (SWG-CA) and requested (Resolution 19 of the Berlin plenary) a joint working group be established in SC21. Conformity assessment for open systems environments is of interest to SC6, SC7, SC18, SC21, SC22, and SC29. As requested by JTC1 in SC21 N 7713, SC21 established [SC21 N 2507] a Joint Working group as WG9 on Conformity Assessment Documentation, with the mandate to publish a technical report based on JTC1 N 2330 as modified by JTC1 N 2303. At the same time, SC21/WG1 developed a new work item proposal for an Open System Assessment Methodology, which was forwarded to JTC1 for a 3-month letter ballot in July 1993. The initial JTC1 ballot [JTC1 N 2612] failed to win support of the required number (5) of national bodies (only CA, GE, IT, and UK promised active participation and resources) [JTC1 N 2773]. (Note: Conformity assessment in connection with conformance testing is addressed in Section 12.2.1.2.)

The liaison statement developed by SC21 and circulated to JTC1, SGFS, EWOS, OIW, and AOW characterizes the work as providing a unifying terminology and general concepts for a methodology and framework for assessment of open systems, covering the following areas:

- ODP, OSE profiles, network management, and APIs
- De facto and de jure standards in coexistence

- Conformance testing and performance testing, and their relationship to interoperability testing, including both active and passive testing (see Section 12.2)
- Use of both testing and specification checking (checking the consistency and mutual compliance of a set of specifications that a system claims to conform to) in order to gain confidence in conformance to the set without having to test against every member of the set
- Points of control and observation not only at communication interfaces, but also APIs, human-computer interfaces, robotic interfaces, and storage media interfaces.

SC21 further noted that the proposed project was clearly of interest to many committees of JTC1 and that it would provide an "umbrella" of common terminology and concepts to inter-link the more detailed testing methodologies of OSI, ODP, POSIX, etc., produced by individual committees. Regional workshops were included because of their interest in OSE profiles. Industry groups, such as the Internet Society, OMG, and X/Open, were also included and proposed as C-liaison organizations.

15.4 Assessment

API standards are needed to specify common methods of accessing network services from programming environments. Examples (from the NIST APP) are:

- API for protocol-independent interfaces. Draft 2, *Detailed Network Interface*, a low-level interface specification, has been completed by IEEE P1003.12. It includes the technology of the XPG4 version of the X/Open Transport Interface and the Version 4.4 BSD sockets interface. It does not yet include features such as the Simple Network Interface and the Naming Interface, which would be included in a later specification.
- Communication API for OSI services. IEEE P1238 has been developing an API between applications and the OSI ACSE and presentation services (but no base document has been agreed); IEEE approval by early 1994 is expected. A separate activity (IEEE P1238.1) is developing an API for FTAM implementations; de facto FTAM API products are available, but the P1238.1 specification is not expected until late 1994.
- Communication API for Integrated Digital, Video, and Voice. An application software interface (ASI) for ISDN is being developed to standardize access and administration of ISDN services (provided by hardware commonly known as network adapters). Version 1 of the ASI was produced by the North American ISDN Users' Forum in June 1992. It contains only a limited set of service definitions. Additional work includes device control and an additional higher level interface.
- Electronic messaging API. An X.400-based electronic messaging API is being developed by IEEE P1224.1 (Draft 3) that defines a language-independent interface between the user of a mail system and the mail system. IEEE approval is expected early in 1993. It does not include EDI and the X.400 Message Store (expected to be treated as addenda to the standard). A high-level API is needed and may be standardized in the future.
- Directory services API. IEEE P1224.2 is developing (Draft 5 was expected in November 1992) a standard directory service user agent interface to support application portability at the source code level. It is language independent and designed to support access to ITU-TS X.500 functionality as well as to other directory services. C language bindings are being specified (P1327.2).

(This page intentionally left blank)

16. INTERNATIONAL AND NATIONAL STANDARDIZED PROFILES

16.1 Profiles of OSI Standards

Quick Reference	
Topic	Page
Assessment	359
CA GOSIP	353
COS/COSINE	359
EPHOS	355
EWOS	345
IGOSS	353
ISODE	358
ISP	342
NATO GOSIP	353
North American OIW	345
OSI Environments	358
POSI	341
Taxonomy of Profiles	343
UK GOSIP	348
US GOSIP	348

The following sections provide examples of the profiles of standards being considered for migration toward open information system environments.

16.1.1 Workshops Developing OSI Profiles

Three regional international workshops have been established to promote OSI. These are the EWOS, POSI (Promoting Conference for OSI)—the Asia/Oceania Workshop (AOW), and the OSE Implementor's Workshop (OIW). The OIW is hosted by NIST. A similar group, IIW (see Section 9.7.6) develops profiles for ISDN.

A Regional Workshop Coordinating Committee has also been established to promote dialog and harmonization among the regional workshops. The goal of the workshops is to define standards profiles that will ensure interoperability of products from different vendors. They are public technical fora organized to provide timely development of implementation agreements and testing details based on international standards. As indicated in Section 16.1.3, the *Stable Implementation Agreements* [Ref. NIST 1991; NIST 1993a] from the OIW form the basis of US GOSIP. A companion document, *Continuing Agreements* [Ref. NIST 1990c], provides the basis for enhancements and future revisions to US GOSIP.

While the current OIW represents a successful model for bringing developers together to identify the additional specificity and precision required to ensure product interoperability, the workshop process may need to change to:

- Include users in an active and visible role of stating requirements and priorities
- Broaden the base of technology providers participating in workshop activities
- More closely align and synchronize assignments, responsibilities, processes and work priorities, and outputs with other regional workshops, user groups, and vendor consortia
- Provide a way for bridging specification gaps with other specifications where appropriate de jure standards do not exist
- Adopt a top-down versus bottom-up approach that reflects a market-driven instead of technology-driven perspective.

At its December 1991 meeting, the OIW adopted, by unanimous vote, a recommendation containing the following points [Ref. Hovey 1992]:

- Revise the charter of the OIW to explicitly state that technical subjects going beyond OSI and into the realm of OSEs can be addressed under the auspices of the OIW.
- Revise the procedures of the OIW to permit the workshop's special interest groups to propose the use of "public domain specifications."

Section 15.1.2.5 describes the work of the OIW Technical Committee on OSE (TC-OSE).

The IEEE Profile Steering Committee, formed in April 1991, has several purposes. It generates, maintains, and interprets profile rules, provides guidance to profile working groups, and provides mechanisms for profile harmonization. Moreover, it effects liaison to related US profile activities, encourages relationships with profile-generating user groups, and effects liaison through appropriate channels to international activities. [Ref. Martin 1992a]

16.1.2 International Standardized Profiles (ISPs)

This section begins by describing the work of the Special Group on Functional Standardization (SGFS) of ISO/IEC JTC1. It then addresses terminology, taxonomy, and issues (Section 16.1.2.2). This is followed by separate sections on application profiles (Section 16.1.2.3), interchange format and representation profiles (Section 16.1.2.4), transport profiles (Section 16.1.2.5), and relay profiles (Section 16.1.2.6). The section ends with a description of the taxonomy of OSE profiles (Section 16.1.2.7).

16.1.2.1 Functional Standardization in ISO/IEC

ISO/IEC JTC1 has set up a Special Group on Functional Standardization (SGFS) to develop standards for international standardized profiles (ISPs). An ISP is somewhat more general than the common use of the term "profile" in that a profile is a stack of protocols to be used in combination, whereas an ISP is a document in which one or more profiles are published. The procedures adopted for specifying ISPs are unique because international harmonization is intended to be achieved before candidate ISPs are submitted to ISO. Proposals for ISPs are expected to be accepted by the international regional workshops EWOS,[77] OIW, and the AOW before becoming proposed draft ISPs (DISPs). SGFS has approved a large number of ISPs, and many others are being discussed in the regional workshops.

The SGFS meets in plenary session in June of each year, 1991-1995. [Ref. SGFS N 242 1991] The scope of the work of the SGFS is the following [Ref. SGFS N 293 1991]:

- Definition of functional standardization and functional standard
- Development of a catalogue of functional standards with appropriate classification
- Definition of a methodology for achieving functional standardization
- Development of a set of operating procedures and assessment of resources
- Execution of the review of proposed draft functional standards
- Consideration of functional standards requirements on conformance and maintenance
- Development of expeditious publication procedures.

A *Directory of ISPs and Profiles Contained Therein* is now SGFS Standing Document SD-4 and accompanies TR 10000 to provide additional information about ISPs and profiles. [SGFS N 100, February 1992] It is currently in its fourth revision and includes:

- Status information about each profile identified in TR 10000
- Summaries of existing or proposed profiles
- Information about the possible joint use of A/B profiles.

16.1.2.2 Functional Standardization Terminology, Taxonomy, and Issues

Terminology. Table 44 provides the definitions of key terms for functional standardization drawn from WDTR 10000-3.

---

[77] A proposed EWOS taxonomy for profiles for open systems environments is given in Section 15.1.3.8.

Table 44. Terminology for International Standardized Profiles

Application Environment (AE) Profile (AEP)—an OSE profile that specifies a complete and coherent subset of the Open System Environment.
Application platform—a set of resources on which an application will run.
Application Program Interface (API)—the interface between the application software and the application platform, across which services are provided.
Component profile—An AE profile that specifies a unit of functionality in terms of the interfaces that it supports and the interfaces that it uses, and the relationships between these interfaces.
Environment (of an information system)—that part of the real world containing the users that exchange messages with the information system.
Interface profile—an OSE profile defining one interface of the OSE.
International Standardized Profile (ISP)—an internationally agreed-to, harmonized document that identifies a standard or group of standards, together with options and parameters, necessary to accomplish a function or set of functions.
Interoperability—the ability of two or more systems to exchange information and to mutually use the information that has been exchanged.
Open System Environment (OSE)—The comprehensive set of interfaces, services, and supporting formats for interoperability and/or for portability of applications, data or people, as specified by information technology standards and profiles.
Portability (software)—the ease with which software can be transferred from one information processing system to another.
Profile (for ISO standardization)—A set of one or more base standards, and, where applicable, the identification of chosen classes, subset, options, and parameters of those base standards, necessary for accomplishing a particular function. Note: An ISP includes the specification of one or more profiles.
Standardization—activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context.
Unit of functionality (UOF)—a separately implementable element of an OSE system.

Taxonomy Framework. The main work of the SGFS is the development of a framework (TR 10000-1), taxonomy for ISPs (TR 10000-2), and principles and taxonomy for OSE profiles (WDTR 10000-3) that gives priority to profiles for OSI but recognizes that the profile principles may also apply to other technical areas. This taxonomy contains a classification and identification scheme for candidate profiles, is being adopted by TSGCE SG9, and will be used in forthcoming editions of the *NATO OSI Profile (NOSIP)*.[78] TR 10000 identifies profiles (specification for how to accomplish a function) and ISPs (harmonized documents). TR 10000 allows an ISP to contain one or more profiles by permitting more than one part, each of which can contain a profile. It is expected that an ISP may contain 5 to 10 profiles. Profiles may only be submitted to the SGFS by one of the three regional workshops (OIW, EWOS, and Asia Oceania Workshop).

Edition 2 of TR 10000-1 remains the agreed text, although Edition 3 is in WD status. TR 10000-2 is in Edition 3. The December 1993 draft of WDTR 10000-2 [SGFS N 1085] has been forwarded by SGFS to JTC1 for DTR balloting [SGFS N 1099 1993]. WDTR 10000-3 is in its first version and there are several key issues to be resolved [Ref. JTFS 92-468 1992]; these are the following:

- Coordination with other groups doing OSE work is needed.
- The relationship between TR 10000-1 and TR 10000-3 is still evolving.
- The relationship between OSE, Application Environment Profiles, and OSI Profiles is still not clear.
- There is no clear understanding of Functional Profiles outside of OSI.

---

[78] SGFS 401, currently in PDTR status, documents the taxonomy update, ISP approval, and maintenance process.

SGFS is now developing procedures to cover other TCs and the OSE. For example, when more that one TC is involved, extra requirements apply such as the generation of a multi-TC ISP memorandum of agreement (MOA) document. [Ref. SC21 N 7360 1992] In December 1993, the SGFS agreed to begin to resolve national body comments on WDTR 10000-1 and 10000-3 by specifying an open system (application platform) that should support application portability but not exchangeability of physical or software components. It was also agreed that interoperability was to be taken as a fundamental requirement, and so the emphasis on application portability should be understood to include both portability and interoperability. [Ref. SGFS N 1099 1993]

In December 1993, SGFS agreed to allow profiles to reference a publicly available specification (PAS) as long as the references are informative (not normative) and as long as the PAS fills an identified gap in the profile for which there is no base standard. The long-term solution to this problem is development of OSE profiles. [Ref. SGFS N 1090 1993]

Issues. SGFS Standing Document SD-7, *Issues List for Future Development of ISO/IEC TR 10000*, September 1993, lists the following current open issues [Ref. SGFS SD-7 1993]:

- Protocol profile testing methodology
- Conformance
- PICS Proforma instructions and Annex C of TR 10000-1
- Profile qualifiers and orthogonal functions
- Terminology: choice between AEP and OSE
- Taxonomy
- Conformance testing of OSE
- Profile versions and ISP revisions
- Cultural elements in ISP and its taxonomies
- Relationship between OSI and OSE
- Scope of OSE profiles
- Call for studies
- Relationship of TR 10000 with ODP
- Taxonomy, profile identifiers, and profiles
- Expansion of the scope of TR 10000-3 to include system software portability.

Related Activities. SGFS has accepted the responsibility for profile test specifications, which will be produced on the same basis as the profile definitions produced by the SGFS [Ref. SC6 N 6976 1991]:

- They will be published as ISPs or ISP parts, related to the ISPs for the profiles to which the tests relate.
- Criteria for inclusion of references to the base standards for relevant abstract test suites will be the same as those for references to PICS proformas.
- Methods of generating and balloting ISPs will be the same as for profiles.

The Regional Workshops Coordinating Committee (RWS-CC) of ISO JTC1 has noted a number of harmonization efforts: conveyance of ODA over MHS(84); FTAM document types from CGM, COBOL, ODA, and EDI; a Document Application Profile (DAP) for raster graphics in ODA; general upper layer agreements; character set repertoires and their encoding; and an international registry (IR) or library (IMIL). [Ref. SGFS N 282 1991]

Table 45 shows the overall organization and labels (taxonomy) used to identify and distinguish ISPs. It shows the distinctions created by the choice of connection-oriented (CO) or connectionless (CL) modes. There are four classes of ISPs in the taxonomy of TR 10000: application profiles (*AXXnn* for those requiring the COTS and *BXXnn* for those requiring CLTS); interchange format and presentation profiles (*FXXnn*); transport profiles (*TXnnnn* and *UXnnnn* for CO and CL profiles, respectively); and relay profiles (.^'' *p,q*).

Table 45. Overview of Taxonomy for International Standardized Profiles

A	Application profiles using CO-mode transport service (TS)
B	Application profiles using CL-mode TS
F	Interchange format and representation profiles
T	Transport profiles providing CO-mode TS
	- TA CO-TS over CL network service (CLNS) using Transport Protocol (TP) Class 4 as defined in ISO 8073/AD 2
	- TB CO-TS over CO network service (CONS) with provision of TP Classes 0, 2, and 4
	- TC CO-TS over CONS with provision of TP Classes 0 and 2
	- TD CO-TS over CONS with provision of TP Class 0
	- TE CO-TS over CONS with provision of TP Class 2
U	Transport profiles providing CL-mode transport service (TS)
	- UA CL-TS over CLNS
	- UB CL-TS over CONS
R	Relay profiles between T- or U-profiles

16.1.2.3 Application Profiles

These profiles are coded by application supported and transport mode required (three letters, where the first letter is "A" if requiring COTS and "B" if requiring CLTS—no *BXX nn* profiles have yet been identified), service type (first digit), and functional association (second digit). The applications are :

- Directory: *ADIn* (e.g., Directory access is ADI1; Directory system is ADI2; distributed operations in ADI3; Directory use of strong authentication is ADI4)
- FTAM: *AFTnn* (e.g., file transfer service is AFT1; file access service is AFT2; file management service is AFT3; filestore management service is AFT4)
- Library, Documentation: *ALDnn* (e.g., search and retrieve is ALD1; interlibrary loan is ALD2)
- MHS: *AMHnn* (e.g., common messaging is AMH1; interpersonal messaging is AMH2; EDI messaging is AMH4)
- MMS: *AMMnn* (e.g., general applications is AMM1; robot controller applications is AMM2; numerical controller applications is AMM3; programmable logic controller applications is AMM4; process industries applications is AMM5)
- OSI Management: *AOMnn* (e.g., management communications is AOM1; management functions is AOM2)
- RDA: *ARD*
- TP: *ATPnn* (e.g., application-supported transactions is ATP1; provider-supported unchained transactions is ATP2; provider-supported chained transactions is ATP3)
- VT: *AVTnn* [e.g., Basic Class (A-mode) is AVT1; Basic Class (S-mode) is ALD2].

Regional workshops (e.g., EWOS, OIW) have defined and ISO/IEC has adopted ISPs for a number of application profiles. These include the following multi-part standards, which are

listed in their entirety (each part and amendments) in Section I.H of Appendix D and Section I of Appendix E:

- ISO/IEC ISP 10607, *ISPs AFT nn - File Transfer, Access, and Management* (Parts 1-6), December 1991
- ISO/IEC ISP 10610, *ISPs FOD nn, Document Structure*
- DISP 10611, *ISPs AMH1n - Message Handling Systems* (Parts 1-5), April 1992
- DISP 10615, *ISPs ADI nn -- OSI Directory* (Parts 1-7), January 1993
- DISP 10616, *ISP FDI 11 - Directory Data Definitions - Common Directory Use,* September 1993
- ISO/IEC ISP 11181, *ISP FOD26 - Enhanced Document Structure - Character, Raster Graphics and Geometric Graphics Content Architecture,* April 1992
- ISO/IEC ISP 11182, *ISP FOD36 - Extended Document Structure - Character, Raster Graphics and Geometric Graphics Content Architecture,* April 1992
- pDISP 11184, *ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles* (Parts 1-7), 1993
- DISP 11185, *ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects* (Parts 1-17), August 1993
- pDISP 11186, *ISPs FVT 3nn - Virtual Terminal Basic Class - Register of Assignment Type Definitions*, 1993
- DISP 11187, *ISPs FVT 3nn - Virtual Terminal Basic Class - Application Profiles* (Parts 1-10), 1993
- pDISP 11188, *ISPs - Common Upper Layer Requirements* (Parts 1-3), July 1993
- DISP 11189, *ISP FDI2 - MHS Use of Directory,* September 1993
- DISP 11190, *ISP FDI3 - FTAM Use of Directory,* September 1993
- DISP 12061, *ISPs ATP nn - OSI Distributed Transaction Processing* (Parts 1-11), July 1993.

Application profiles for OSI management adopted by ISO/IEC are the following:

- ISO/IEC ISP 11183, *ISPs AOM 1n - OSI Management - Management Communications Protocols* (Parts 1-3), December 1992
- DISP 12059, *ISPs - Management Functions - Common Information for Management Functions* (Parts 0-6), 1992
- DISP 12060, *ISPs AOMnnn - OSI Management - Management Functions* (Parts 1-5), 1992.

16.1.2.4 Interchange Format and Representation Profiles

ISPs for interchange formats and representations are coded by information type (three letters), document structure (first digit), and architecture (second digit). The information types are (the last two have no two-digit extensions):

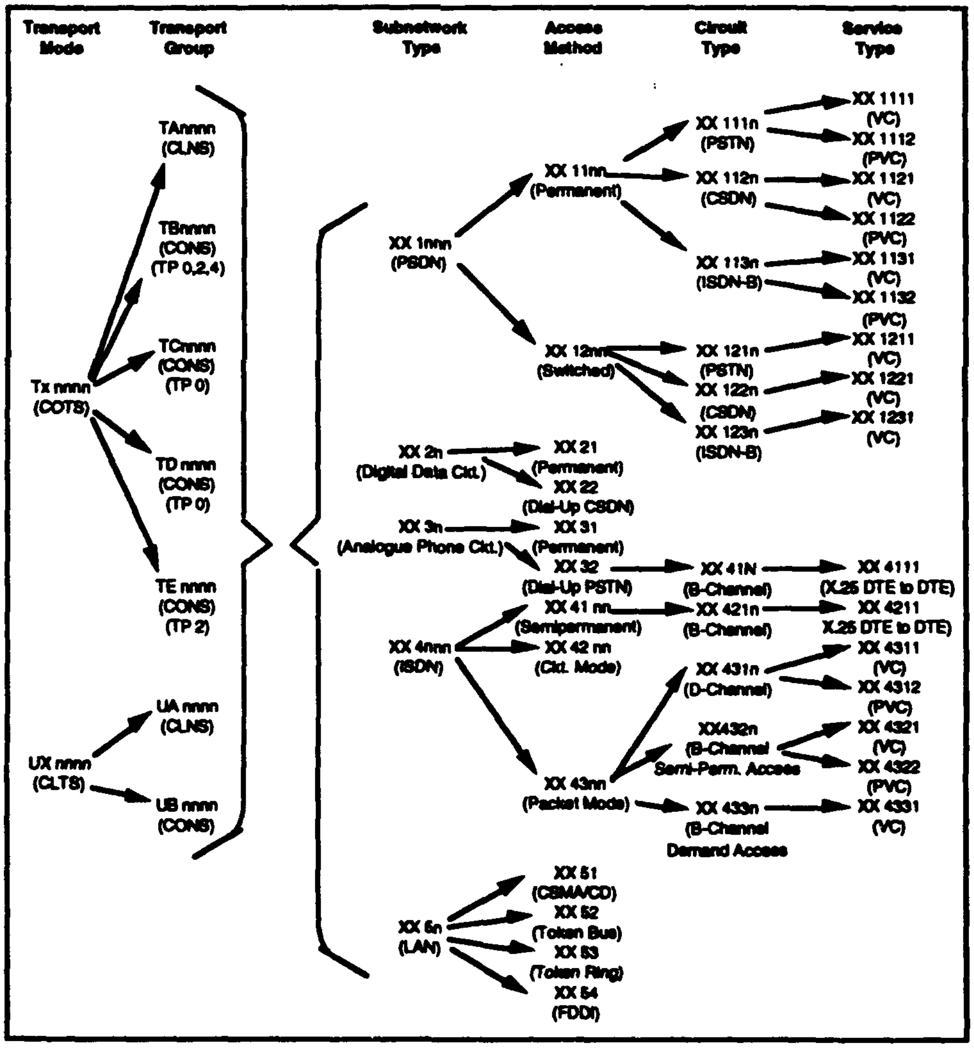
- Computer graphics: *FCGnn*
- Directory data definitions: *FDInn* (e.g., common Directory use is FOD1; MHS use of Directory is FDI2; FTAM use of Directory is FDI3)
- Office document: *FODnnn* (e.g., document processing applications is FOD0; image applications is FOD1)
- SGML document: *FSGnn*
- Virtual terminal control objects: *FVTnn.*

Section 7.1.1 lists the office document profiles under development. Section 5.2.3 lists the VT profiles under development. Section 9.11.7.5 lists the Directory profiles under development.

16.1.2.5 Transport Profiles

Transport profiles (Figure 18) are coded by transport mode (first letter "T" for COTS and "U" for CLTS), transport group (second letter), subnetwork type (first digit), access method (second digit), circuit type (third digit), and service type (fourth digit). The transport groups are CLNS (*TA* or *UA*), TP 0/2/4 over CONS (*TB* or *UB*), TP 0/2 over CONS (*TC*), TP0 over CONS (*TD*), and TP2 over CONS (*TE*). The subnetwork types are PSDN ("1"), digital data circuit ("2"), analog telephone circuit ("3"), ISDN ("4"), and LAN ("5"). The access methods differ for circuits and LANs:

- Circuit access: permanent ("1"), switched ("2"), and packet mode ("3")
- LAN access: CSMA/CD ("1"), token bus ("2"), token ring ("3"), and FDDI ("4").



Source: [Ref. Onufer 1990]

Figure 18. Taxonomy for International Standard Transport P.ofiles

Transport profiles defined by regional workshops and adopted by ISO/IEC include the following multi-part standards, which are listed in their entirety (each part and amendment) in Section I.H of Appendix D and Section I of Appendix E:

- ISO/IEC ISP 10608, *ISPs TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service* (Parts 1-14), 1992
- ISO/IEC ISP 10609, *ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service* (Parts 1-38), 1992.

16.1.2.6 Relay Profiles

These profiles are coded by relay type:

- CLNS: *RAp,q*
- CONS: *RBp,q*
- X.25: *RCp,q*
- MAC using transport bridging: *RDp,q*
- MAC using source routing: *REp,q*
- CLNS to CONS: *RZp,q.*

The four-digit numbers p and q each use the four-digit numerical classification of the transport profiles. They thereby identify the subnetwork types between which the relay occurs.

Relay profiles defined by regional workshops and adopted by ISO/IEC include the following multi-part standards, which are listed in their entirety (each part and amendment) in Section I.H of Appendix D and Section I of Appendix E:

- DISP 10612, *ISPs RD nn.nn* (Parts 1-9), 1993
- DISP 10613, *ISPs RA nn.nn - Relaying the Connectionless-mode Network Service* (Parts 1-9), 1993
- DISP 10614, *ISPs RC nn.nn - Relaying X.25 PLP* (Parts 1-6), 1993.

16.1.2.7 Open System Environment Profiles

Table 46 identifies the taxonomy of OSE profiles included in the current draft of WTR 10000-2.4 and WDTR 10000-3. Note that there are two classes of these profiles: application environment profiles and interface profiles.

16.1.3 National and Multinational GOSIPs

16.1.3.1 UK and US GOSIP

This section discusses UK GOSIP and US GOSIP, illustrated side by side in Figures 19 and 20. Documentation for UK GOSIP was originally issued in March 1988 for mandatory use in 1990. It is now in Version 4. [Ref. OSN 1991i, 19] Figure 19 shows the standards recommended for UK GOSIP. Documents for Version 4 of UK GOSIP, *UK Government OSI Profile*, are [Ref. CCTA 1992a; CCTA 1992b]:

- Volume I, *Introduction*
- Volume II, *Specification*
- Volume III, *Procurement Handbook.*

Previously, UK GOSIP was completely revised and updated on an annual basis. Now the life span of the new GOSIP 4 document sets is expected to be 2-3 years, which will allow periodic updates to be added into the new ring-binder format. [Ref. OSN 1991m]

Table 46. Example Taxonomy for Application Environment Profiles

P	OSE Profiles					
	AEP	AEP Profiles				
		PC	Component Profiles			
		PS	System Profiles			
			PSB	Base Environment Profiles		
				PSB1	Generic Base Environment	
				PSB2	... (to be extended if necessary)	
			PSE	Generic Environment Profiles		
				PSE1	Workstation Environments	
					PSE10	Terminal Environment
					PSE11	Personal Workstation Environment
					PSE12	Professional Workstation Environment
				PSE2	Utility Server Environments	
					PSE20	Electronic Message Serving Environment
					PSE21	Directory Serving Environment
					PSE22	Access Control Serving Environment
				PSE3	Information Server Environments	
					PSE30	DBMS Serving Environment
					PSE31	Document Serving Environment
				PSE4	Transaction Processing Environments	
					PSE40	Simple TP Environment
					PSE41	Enhanced TP Environment
				PSE5	Real-Time Environments	
					PSE50	Real-Time Environment, seconds
					PSE51	Real-Time Environment, milliseconds
				PSE6	Supercomputing Environments	
	IP	Interface Profiles				
		HCI	Human-Computer Interface			
		CMI	Communication Interface			
		ISI	Information Interface			
		API	Application Program Interface			

Rather than repeat UK GOSIP, Canada has prepared *Canadian Open Systems Applications Criteria (COSAC)* as a Government strategy toward open systems. The strategy is analogous to UK GOSIP and fully subscribes to ISO conventions. The mandate of the Department of National Defence in Canada is to follow COSAC (i.e., UK GOSIP) where defined and otherwise to revert to ISO open systems specifications. Canada does not plan to develop a national, made-in-Canada open system architecture. [Ref. Beggs 1992]

Figure 20 shows the standards and options recommended for US GOSIP, Version 2.0. [Ref. GOSIP 1990] These are based on the March 1990 *Stable Implementation Agreements for Open Systems Interconnection Protocols,* Version 3, Edition 1, of the OIW [Ref. NIST 1990b] Version 1.0 was issued as FIPS 146 on August 1989. Version 2.0 was issued as FIPS 146-1 on October 1990. Use of FIPS 146 was mandatory August 1990, and FIPS 146-1 became mandatory on October 1991.

Whereas in Version 1.0 of US GOSIP only the CL-mode network layer protocols were recommended for packet switched wide area networks (WANs), Version 2.0 makes CO-mode network service optional. This, and the addition of the Network Service Access Point (NSAP) address structure, will align the standard with those currently being addressed by ISO.

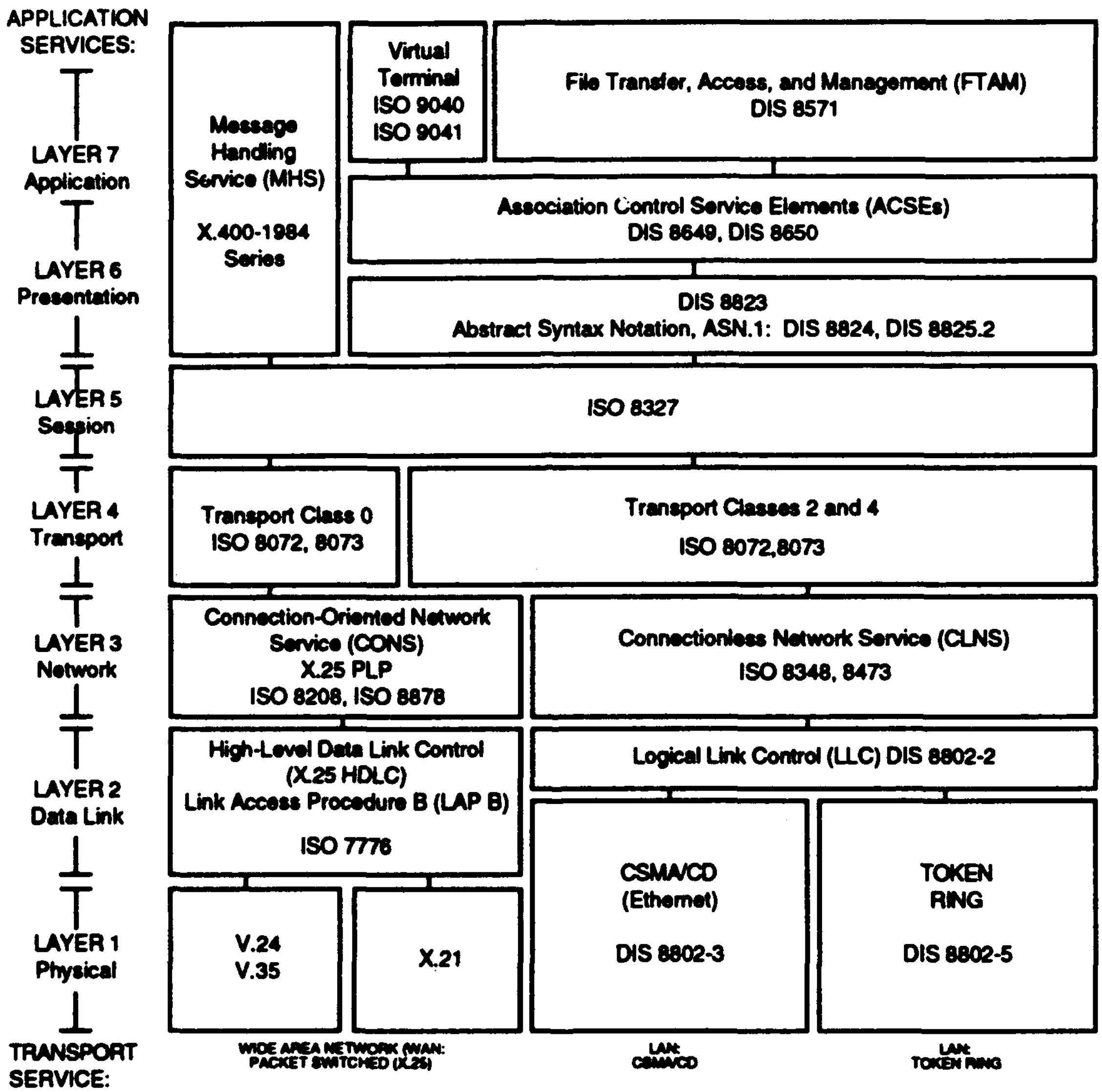


Figure 19. Stacks of Standards Recommended for UK GOSIP

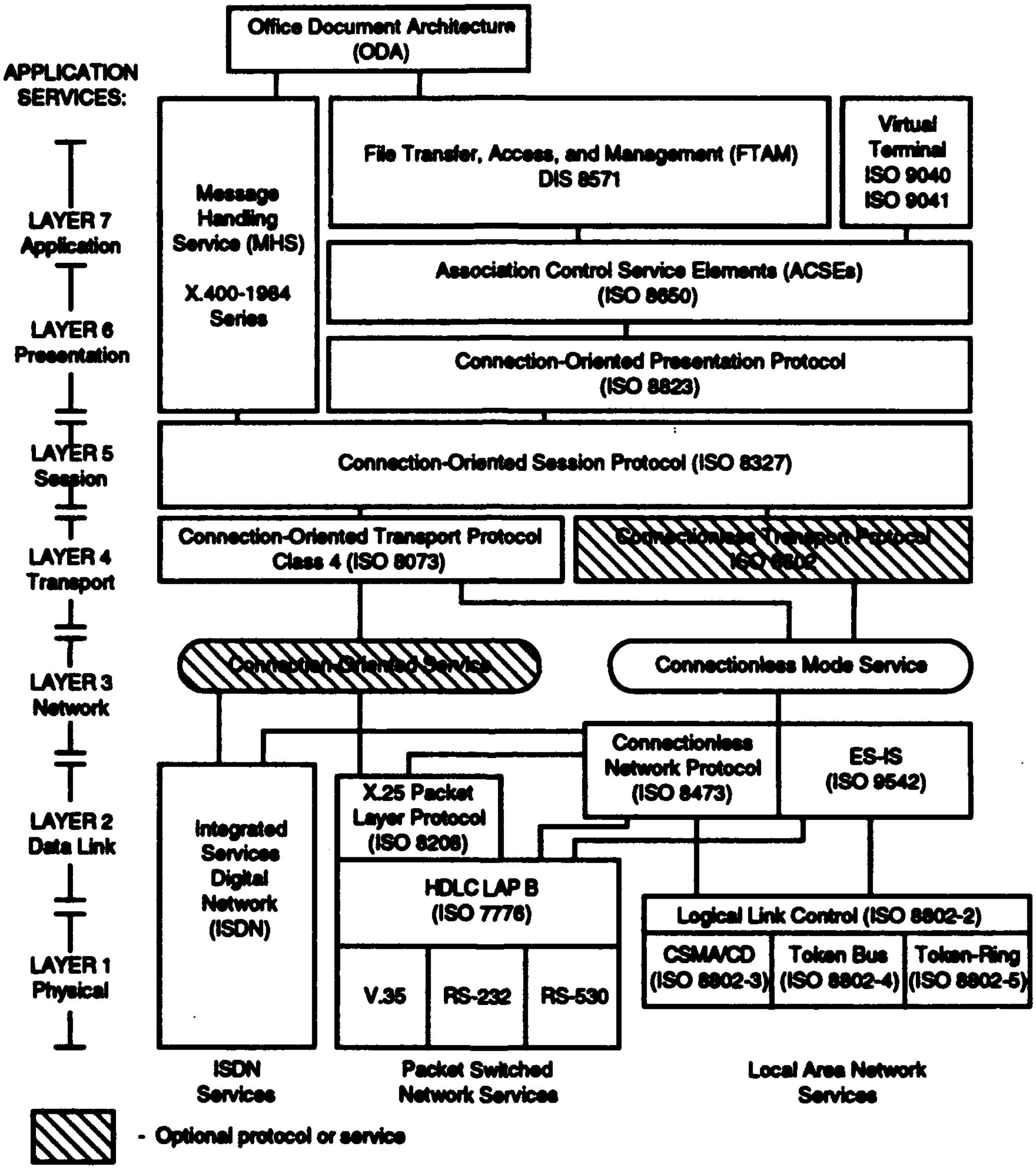


Figure 20. Stacks of Standards Recommended for US GOSIP (Version 2.0)

Versions of US GOSIP will continue to be based on the stable implementation agreements reached in the regional OSI Implementor's Workshop. Working agreements from the OIW that have not reached final form are found in the *Working Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements.* These agreements provide the basis for future projections of US GOSIP.

In addition to recognizing, including, and resolving Version 1.0 errata, Version 2.0 of US GOSIP [Ref. GOSIP 1990], also includes the following protocols: VT (forms profiles and TELNET), ODA/ODIF, ISDN, connection-oriented network service, connectionless transport, and end-system to intermediate system (ES-IS) network layer protocols. These protocols would be added in Version 3.0, which is planned for 1995: Directory services (ITU-TS X.500), VT (page, scroll, and forms), 1988 ITU-TS extensions to MHS, FTAM extensions, FDDI, optional Transport Class 2, Computer Graphics Metafile, MMS, network management, optional security enhancements, SGML, EDI, and intra-domain routing protocols. Version 4.0, planned for 1997, will include transaction processing (TP), remote database access (RDA), additional network management, additional optional security, and inter-domain routing protocols. [Ref. OSN 1991e, p.4]

A detailed description of the plans, based on US GOSIP, to introduce OSI protocols into the US DoD is provided in *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy*. [Ref. MITRE 1988] The baseline for US tactical implementation of OSI standards and protocols will be based on the work of TSGCE SG9, the *NTIS Transition Strategy*, and associated STANAGs. Tactical networks may use GOSIP-specified lower-level protocols until NTIS protocols are developed and commercially available. When the NATO standards are complete, approved, and available, those required for DoD use will be introduced as GOSIP Advanced (post-1989) Requirements. [Ref. MITRE 1988]

While some major vendors such as IBM are offering (or about to offer) OSI for much or all of their product line, they are typically offering TCP/IP as well. The August 1990 US GOSIP mandate seems to have influenced the schedule for many of the OSI implementors, so a number of first generation OSI products either are just appearing or expected shortly. Activity in the TCP/IP product lines is undiminished. [Ref. PSSG 1991]

NIST is publishing a series of US GOSIP evaluation guidelines that are now available for electronic mail and transfer. These guidelines explain how implementations can differ, and they assist Federal agencies and other users in determining which among several implementations best suits their needs. [Ref. OSN 1991e, 5]

Since Version 3.0 of US GOSIP will be introducing standardized network management, an important area where a lot of standards work remains to be done, NIST is developing a number of FIPS concerning network management. They will be published in stages, one each year for the next three years, and will describe the objects that have to be managed to perform network management or OSI management in the following functional areas:

- Phase I: 802, X.25, ISDN, FDDI, modems, multiplexes, bridges, and physical link
- Phase II: protocol software, routers, terminal services, MTAs, PBXs, and circuit switches
- Phase III: applications, services, operating systems, computer networks, and DBMSs.

The staging of these FIPS reflects user priorities. In a survey of Federal agencies, NIST found that the most important area is management for local area networks and Layers 1 and 2 of the OSI Reference Model. Next were Layers 3-7 and then network management applying to operating systems, applications, and services. [Ref. OSN 1991e, 7]

16.1.3.2 NOSIP

Subgroup 9 of NATO's TSGCE has recently released Version 3 of the *NATO Open Systems Interconnection Profile (NOSIP) Strategy* [Ref. NATO 1993]. This document identifies a number of international standards as base standards and emerging international profiles for use in NATO systems. Appendixes D and E identify each standard listed and profile included in the *NOSIP Strategy.* The following (draft) STANAGs are under development as military profiles based on international standards:

- STANAG 4406, *Military Message Handling System,* Draft, NATO UNCLASSIFIED (cf. ISO 10021, 10611)
- STANAG 4407, *System Management,* Draft, NATO UNCLASSIFIED (cf. ISO 10165-1, 10165-2, 10165-4, 10164, 11183, 12059, 12060)
- STANAG 4408, *Connection-mode Transport Service over Connectionless-mode Network Service* (Parts 1-4)
- STANAG 4409, *Connection-mode Transport Service over Connection-mode Network Service (Military)* (Parts 1-3)
- STANAG 4410, *Connectionless-mode Transport Service over Connectionless-mode Network Service*
- STANAG 4413, *Relaying the Connectionless-mode Network Service* (Parts 1-4).

16.1.3.3 Multinational GOSIP—IGOSS[79]

The Industry/Government Open Systems Specification (IGOSS) [Ref. IGOSS 1993] is jointly authored by the US Government, the Canadian Government, MAP Users Group, TOP Users Group, and the Electric Power Research Institute (EPRI). Each of these five major user organizations have issued their own procurement profiles to coordinate the acquisition and operation of computer networking products and services based on OSI standards. In the future, these organizations intend to specify OSI profiles (e.g., GOSIP) primarily by reference to IGOSS in future editions of such documents as the following:

- Canadian Open System Application Criteria (COSAC) [to be issued as a Treasury Board Information Technology Standard (TBITS)]
- MAP specification
- TOP specification (see Section 15.1.3.6)
- US GOSIP [to be issued as a Federal Information Processing Standard (FIPS)]
- Utility Communications Architecture.

IGOSS defines profiles for the following:

- Message Handling Systems (ITU-TS 1988 Recommendations)
- Electronic Data Interchange (EDI) User Agent
- File Transfer, Access, and Management (FTAM)
- Virtual Terminal Service, Remote Database Access, and Transaction Processing
- Directory service

[79] The material for this section is excerpted from [IGOSS 1993].

- Manufacturing Message Specification (MMS)
- X-Windows over OSI
- Information retrieval
- Fiber Distributed Data Interface (FDDI)
- Frame relay
- Point-to-Point Protocol (PPP)
- Intermediate System to Intermediate System (IS-IS) Routing Protocol
- Inter-Domain Routing Protocol (IDRP)
- Network management protocols
- Connectionless Upper Layer services.

The primary sources for IGOSS are ISPs and the stable implementation agreements from the North American OIW. Secondary sources (in order of precedence) are international standards and recommendations from ISO and ITU-TS; draft international standards; IEEE standards; and working implementation agreements from the OIW. In some cases, IGOSS makes reference to tertiary sources, which are (in order of precedence): ANSI standards; Canadian Standards Association standards; committee draft international standards; FIPSs; CTBITS; Internet standards and requests for comment (RFCs); and military standards.

IGOSS defines application subprofiles, lower-layer subprofiles, and subnetwork subprofiles. These subprofiles are combined to provide product specifications for procurement. An overview of these subprofiles is provided in Figure 21. Application subprofiles in IGOSS are summarized in Table 47 and transport and relay profiles in Table 48.

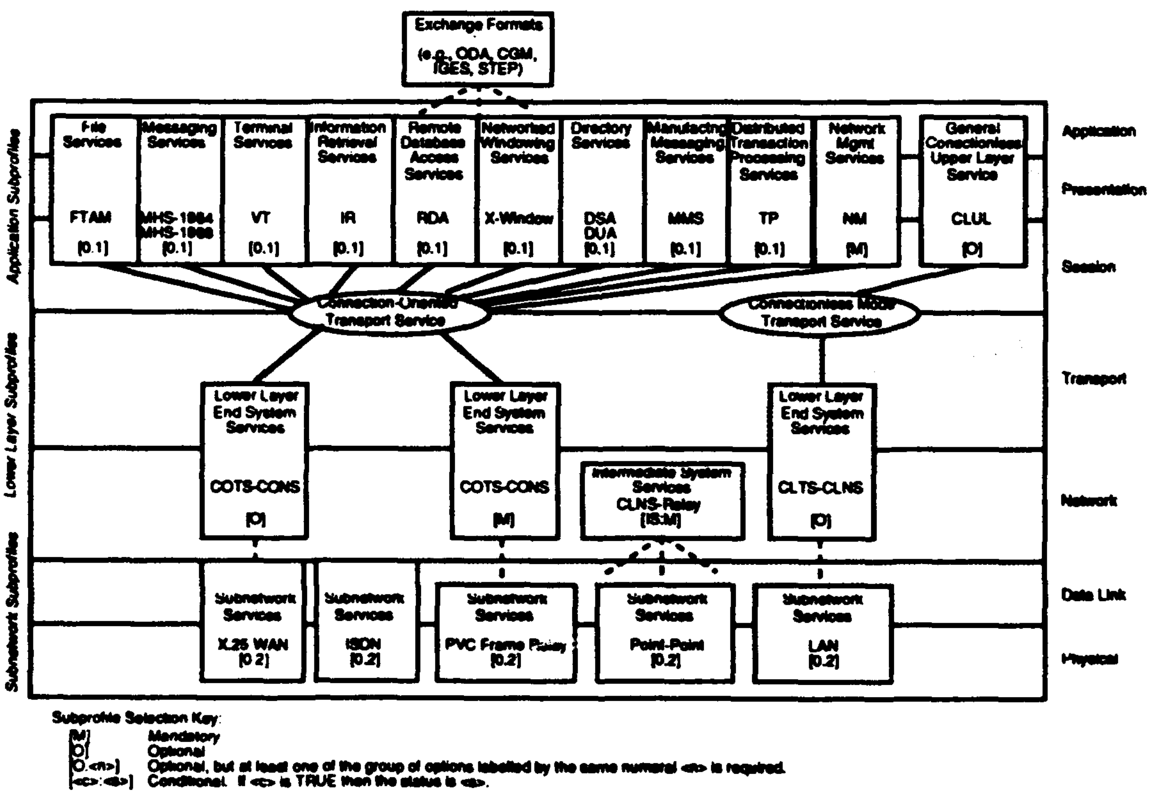


Figure 21. IGOSS Subprofiles

Table 47. IGOSS Application Subprofiles

Subprofile	Standards for the Subprofile			
	Layer 5	Layer 6	Layer 7 Application Service Elements	Layer 7 Applications
FTAM	ISO 8327	ISO 8823	ISO 8650 (ACSE)	ISO 8571-4
MHS-88	ISO 8327	ISO 8823	ISO 8650 (ACSE) ISO 9066-2 (RTSE) ISO 9072-2 (ROSE)	ITU-TS X.400:1988
MHS-884	ISO 8327	(Null)	ITU-TS X.410 (RTS)	ITU-TS X.400:1984
VT	ISO 8327	ISO 8823	ISO 8650 (ACSE) ISO 9805 (CCR) ISO 10026 (TP User ASE)	ISO 10026-3
TP	ISO 8327	ISO 8823	ISO 8650 (ACSE)	ISO 8571-4
RDA	ISO 8327	ISO 8823	ISO 8650 (ACSE)	ISO 9579
Directory	ISO 8327	ISO 8823	ISO 8650 (ACSE) ISO 9066-2 (RTSE) ISO 9072-2 (ROSE)	ISO 9594 (ITU-TS X.500)
MMS	ISO 8327	ISO 8823	ISO 8650 (ACSE)	ISO 9506
CMIP	ISO 8327	ISO 8823	ISO 8650 (ACSE) ISO 9072-2 (ROSE)	ISO 9596-1
X-Windows	ISO 8327	ISO 8823	ISO 8650 (ACSE)	ANSI S.3-219-199x
Information Retrieval	ISO 8327	ISO 8823	ISO 8650 (ACSE)	ISO 10163 or ANSI Z39.50
Connectionless	ISO 9548	ISO 9576	ISO 10035 (ACSE)	(User Application)

Source: [IGOSS 1993]

Table 48. IGOSS Transport and Relay Subprofiles

Subprofile	Standards for the Subprofile			
	Layer 1	Layer 1	Layer 3	Layer 4
COTS-CLNS	(Null)	(Null)	ISO 8348, 8348/AD1 (CLNS) ISO 8473 (CLNP) ISO 9542 (ES-IS Routing Protocol)	ISO 8072 (COTS) ISO 8073, 8073/AD1 (COTP)
COTS-CONS	(Null)	(Null)	ISO 8348 (CONS) ISO 8878 (Use of X.25 to Provide CONS) ISO 10030 (ES-IS Routing Protocol)	ISO 8072 (COTS) ISO 8073 (COTP), Classes 4, 2, and 0
CLTS-CLNS	(Null)	(Null)	ISO 8348, 8348/AD1 (CLNS) ISO 8473 (CLNP) ISO 9542 (ES-IS Routing Protocol)	ISO 8072, 8072/AD1 (CLTS) ISO 8602 (CLTP)

Source: [IGOSS 1993]

16.1.4 European Procurement Handbook for Open Systems (EPHOS)

Decision 87/95 from the European Community (EC) requires the specification of OSI standards for public procurements. A document is being developed by France, Germany, and the United Kingdom to provide guidance for such procurements. The document is called the European Procurement Handbook for Open Systems (EPHOS) and is based on base profiles of the UK GOSIP specification. Where possible, EPHOS will cite European standards and ISPs.

In early 1991, EPHOS achieved two significant milestones. The Phase I draft covering X.25, MHS, and FTAM now reflects member nations' formal comments, and Phase II has progressed to the point of agreement on further coverage. The original intention to publish procurement guidance on MHS-88 has been undermined by slow progress on the European standards, and EPHOS Phase I has been revised to focus on MHS-84 with only preliminary

guidance on specifying MHS-88 added functionality. Phase II topics will include: Phase I maintenance, FTAM, MHS-88, LAN, cabling, document formats, character repertories, Security, EDI, directory services, VT, LAN/WAN interworking, and identification of areas where standards are inadequate or absent. [Ref. OSN 1991g]

16.1.5 International Versions of GOSIP

Initiatives have been taken to develop an international version of GOSIP. The initial meeting in October 1988 was sponsored by the United Kingdom, with participation from France, Germany, Canada, Japan, Sweden, and the United States.

16.1.6 US Military Standardized Profiles for Open Systems

The US DTMP is developing a number of Defense Standardized Profiles (DSPs) that meet US military requirements and that could be submitted to TSGCE SG9 to be considered as potential NATO Standardized Profiles. Table 49 shows the status of DTMP profile development as of January 1994. These are listed with full titles along with other national military standards and profiles in Section II.B of Appendix H.

Table 49. US Defense Standardized Profile Development

3500-Series—Network/Relay Profiles/Multi-Layer
MIL-STD-1745-13500, Internet Relay Profile for DoD Communications - Point-to-Point Protocol (PPP), Working Draft, Draft, 1993
4500-Series—Transport Profiles/Multi-Layer
MIL-STD-1745-14500, DSPs - Reliable End System (ES) Transport for DoD Communications, Draft, 1993 (approved by DTMP for validation)
MIL-STD-1745-14501, DSPs - Simplex Transport Profile (in SD-1 coordination[80])
MIL-STD-1745-14502-01, DSPs - Internet Transport Profile for DoD Communications, Part 1: Transport and Internet Services, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-14502-02, DSPs - Internet Transport Profile for DoD Communications, Part 2: Point-to-Point Links, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-14502-03, DSPs - Internet Transport Profile for DoD Communications, Part 3: Wide Area Network Access, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-14502-04, DSPs - Internet Transport Profile for DoD Communications, Part 4: Local Area Network (LAN) Media Independent Requirements, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-14502-05, DSPs - Internet Transport Profile for DoD Communications, Part 5: Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) Local Area Network (LAN) Media Dependent Requirements, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-14502-06, DSPs - Internet Transport Profile for DoD Communications, Part 6: Combat Net Radio, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-44500, Tactical Communications 2 (TACO2), Draft, 1993 (sent to Navy publications)
7500-Series—Application Profiles/Multi-Layer
MIL-STD-1745-17501-01, DSPs AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 1: MHS Service Support, Draft, 1993 (sent to Navy publications)
MIL-STD-1745-17501-02, DSPs AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by DoD MHS, Draft, 1993 (sent to Navy publications)

80 Standardization Directory (SD-1) coordination is conducted to provide a baseline (incorporating comments from SD-1 coordination) for formal validation prior to final approval and publication.

Table 49. (Cont'd)

MIL-STD-1745-17501-03, DSPs AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 3: Requirements for Message Transfer (P1), Draft, 1993 (sent to Navy publications)
MIL-STD-1745-17501-04, DSPs AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 4: Messaging Requirements for MTS Access (P3), Draft, 1993 (sent to Navy publications)
MIL-STD-1745-17501-05, DSPs AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 5: Messaging Requirements for MS Access (P7), Draft, 1993 (sent to Navy publications)
MIL-STD-1745-17502, MHS Military Messaging, Content Type AMH 2n (D), Draft, 1993 (baseline for validation; requesting approval to publish from DTMP)
MIL-STD-1745-17503-01, DSPs - Internet Message Transfer Profile for DoD Communications, Part 1: Simple Mail Transfer Protocol (in SD-1 coordination)
MIL-STD-1745-17503-02, DSPs - Internet Message Transfer Profile for DoD Communications, Part 2: Format of Text Messages, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17504, DSPs - Internet File Transfer Profile for DoD Communications, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17505, DSPs - Internet Domain Name Service (DNS) Profile for DoD Communications, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17506, DSPs - Internet Remote Login Profile for DoD Communications, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17507-01, DSPs - Internet Network Management Profile for DoD Communications, Part 1: Simple Network Management Protocol (SNMP), Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17507-02, DSPs - Internet Network Management Profile for DoD Communications, Part 2: Management Information Base (MIB), Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17507-03, DSPs - Internet Network Management Profile for DoD Communications, Part 3: Structure and Identification of Management Information, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17508-01, DSPs AFT 1n (D) - File Transfer, Access and Management, Part 1: Specification of ACSE, Presentation and Session Protocols for Use by FTAM, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17508-02, DSPs AFT 1n (D) - File Transfer, Access and Management, Part 2: Definition of Document Types, Constraint Sets and Syntaxes, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17508-03, DSPs AFT 1n (D) - File Transfer, Access and Management, Part 3: AFT 11—Simple File Transfer Service (Unstructured), Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17508-04, DSPs AFT 1n (D) - File Transfer, Access and Management, Part 4: AFT 12—Positional File Transfer Service for Flat Files, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17508-05, Information Technology - Defense Standardized Profiles AFT 1n (D) - File Transfer, Access and Management, Part 5: AFT 22—Positional File Access Service for Flat Files, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-17508-06, DSPs AFT 1n (D) - File Transfer, Access and Management, Part 6: AFT 3—File Management Service, Draft, 1993 (in SD-1 coordination)
8000-Series—Network Management
MIL-STD-1745-38000, Government Network Management Profile (GNMP), 1991 (approved and published)
MIL-STD-1745-38000, DoD Network Management for DoD Communications, Version 2 of GNMP, Draft (working group circulation), DTMP/WG3, 1992
8500-Series—Security
MIL-STD-1745-18500-01, DSPs AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 1: MSP Service Support, Draft, DTMP/WG3, 1993 (sent to Navy publications)
MIL-STD-1745-18500-02, DSPs AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 2: MSP Content Protocol, Draft, DTMP/WG3, 1993 (sent to Navy publications)
MIL-STD-1745-18500-03, DSPs AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 3: MSP Requirements for Message Transfer, Draft, DTMP/WG3, 1993 (sent to Navy publications)
MIL-STD-1745-18500-04, DSPs AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 4: MSP Requirements for MS Access, Draft, DTMP/WG3, 1993 (sent to Navy publications)
MIL-STD-1745-18500-05, DSPs AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 5: MSP Requirements for MS Access, Draft, DTMP/WG3, 1993 (sent to Navy publications)
MIL-STD-1745-48501, Common Security Label, Draft, 1993 (in SD-1 coordination)

Source: [Curcio 1994]

16.1.7 Other Profiles and Transition Strategies

This section is intended to be expanded to address additional activities and options to support transition from existing military and other standards to standards for open environments.

Examples are application gateways, test systems, and test methodologies. Efforts to highlight functional standards, select stacks of mature standards and options within standards, and harmonize implementations will be examined. One example is the *Guide to the Use of Standards* [Ref. SPAG 1987] developed by SPAG in Europe. Functional standards based on OSI standards are being developed by the Interoperability Technology Association for Information Processing, Japan (INTAP), specifically towards an interoperable distributed database system. [Ref. Konoike 1987] Recommendations for functional standards and cooperation with European and US organizations and companies are also provided in Japan by POSI.

16.1.8 US Policy on Coexistence and Convergence of TCP/IP-OSI

At the request of the Office of Management and Budget (OMB) in collaboration with the Federal Networking Council and Federal Information Resources Management Policy Council, NIST established the Federal Internetworking Requirements Panel (FIRP) to reassess federal requirements for open systems networks and to recommend policy on the Government's use of networking standards, specifically on the coexistence of TCP/IP and OSI. FIRP's draft report [Ref. FIRP 1994] concluded that no single protocol suite meets the full range of government requirements for data internetworking and makes five recommendations:

- The role of oversight and integration across federal agency internetworking activities should be strengthened within the OMB.
- The roles and responsibilities for fostering standards and assessing technological change should be refocused and strengthened by the Department of Commerce.
- The roles and responsibilities for infrastructure development and operations to support all internetworking services from advanced research and development to leading edge to core/commodity services should be clearly defined and formally assigned through the Information Infrastructure Task Force
- The roles and responsibilities of affinity groups should be defined, including how they are created and coordinated by the Government Information Technology Services working group.
- In accordance with OMB Circular A-119, Revised October 1993, voluntary standards should be adopted and used by Federal agencies, and international standards should be considered in the interests of promoting trade. The current GOSIP policy should be modified by the Department of Commerce to reflect the wider range of international voluntary standards for internetworking.

16.2 OSI Environments

16.2.1 ISO Development Environment (ISODE)

ISODE is prototype software, developed as a tool to study OSI. However, in the current vacuum of OSI implementations, ISODE has become a default reference implementation of the OSI upper-layers, a platform for deploying OSI services, and a means for transitioning from TCP/IP to OSI protocols.

The ISODE software supports various OSI protocols and applications. ISODE is aligned with US GOSIP. The current modules include the following [Ref. Rose 1990]:

- OSI transport service (TP0 on top of TCP, X.25, and the CO network service; TP4 for SunLink OSI)
- OSI session, presentation, and association control services
- ASN.1 abstract syntax/transfer notation tools

- OSI reliable transfer and remote operations services
- FTAM/FTP gateway
- OSI Directory services
- OSI VT (basic class and TELNET profile).

The ISODE Consortium (see Appendix F, Section 3.28) was formed in 1992 to take charge of further development of ISODE and to commercialize it. [Ref. OSN 1992o]

16.2.2 COS/COSINE Recommendations

Initial profiles for Corporation for Open Systems Interconnection in Europe (COSINE) have been released. These profiles are summarized in Table 50. In addition to those standards cited in the table, COSINE is evaluating:

- Virtual Terminal, ISO 9041 (with AD2 screen mode)
- EWOS Profile A/122 for file access
- Additional message handling services (ITU-TS X.400-1988)
- Job Transfer and Manipulation (JTM), ISO 8832 and ISO 8833.

Table 50. Standards for COSINE Profiles

Layer	References for Standards
7. Application	ENV 41204 (FTAM) ENV 41910 (Remote Terminal Access) EWOS Profile A/111 (File Access) RARE MHS and ITU-TS X.400-1984 MHS Services Rem[illegible] Job Entry (to be defined in EWOS)
6. Presentation	(Null Layer)
5. Session	(Null Layer)
4. Transport	(Connection-Oriented)
3. Network	(Connection-Oriented)
2. Data Link	ITU-TS X.25-1984
1. Physical	Local Area Networks (not specified)

16.3 Assessment of Coverage by Standards

Findings related to standardized profiles for communications services are the following:

- Lack of capability to cross between connection-oriented and connectionless-mode services in OSI profiles. The OSI Reference Model has been revised to incorporate connectionless services (previously treated as an addendum). Most work on crossover is being addressed by transport or relay bridges, some of which do not conform to the Reference Model. This is a major problem for interoperability between North America (which uses predominantly connectionless modes) and Eu[illegible]e (which uses predominantly connection-oriented modes). As an example, U[illegible] [illegible] UK GOSIP are not compatible and no progress has been made to converge these efforts. However, Version 2.0 of US GOSIP includes an optional connectionless transport service and an optional connection-oriented network service for use on end-systems connected to X.25 networks that are not going to be connected to local area networks.
- Few international standardized profiles (ISPs) have been adopted by ISO. Work on FTAM profiles is the most mature and three of the FTAM ISPs have been adopted by ISO. EWOS is preparing a number of candidates for adoption in ISO, but these emphasize connection-oriented services. Profile work in NIST is progressing rapidly,

but the products are not yet in the form that can be used for an ISP. Adoption of common ISPs is critical to the compatibility of products based on OSI and other open system protocols.

17. STATUS OF NATO OPEN SYSTEM DATA DISTRIBUTION STANDARDS

17.1 Introduction

This chapter and the next examine NATO efforts to analyze, specify, and implement open system standards and architectures to achieve interoperability. The purpose is to (1) assess the progress being made in NATO to incorporate military requirements in international standards and to define, where necessary, extensions to those standards, and (2) identify the NATO standards and profiles that may be applicable to ATCCIS (and other CCISs). Chapter 17 focuses on data distribution and therefore on the work of TSGCE Subgroup 9 (SG9). Chapter 18 addresses analyses, demonstrations, tests, development, and other initiatives for data communications and information systems to achieve interoperability and cost savings through multinational cooperation. National initiatives in these areas are addressed in Chapter 19.

This section is followed by a discussion of the eight military requirements defined by TSGCE SG9 (Section 17.2) and an overview of SG9's organization and the plans and activities of the working groups (WGs) within SG9 (Section 17.3). Section 17.4 assesses the status of draft OSI STANAGs. The chapter concludes with a summary of related standards work in NATO bodies (Section 17.5) and the overall assessment (Section 17.6).

17.2 Military Requirements for NATO OSI

This section summarizes the requirements associated with incorporating military enhancements into open systems interconnection (OSI) standards. Within NATO, this work has been assigned to TSGCE SG9. General information on NATO and international standards bodies concerned with OSI standards is provided in Appendix F.

Beginning in February 1983, a number of military requirements have been identified in NATO that are not adequately covered by all existing OSI standards. Eight military features were identified in the NATO Interoperability Management Plan (NIMP) [Ref. NIMP 1988], and TSGCE SG9 has recommended that the OSI Reference Model (STANAG 4250) be extended to provide support for these features:

- Multihomed, mobile host systems
- Multi-endpoint connection
- Internetworking
- Network/system management functions
- Security

- Robustness and quality of service
- Precedence and preemption
- Real-time and tactical communications.

Table 51 gives the description of the eight military features[81] as provided in *Use of OSI Standards in NATO—Strategic and Technical Issues*, March 1988. [Ref. UK 1988]

Table 51. Eight Military Features for Enhancing OSI in NATO

(1)	Multihomed and mobile host systems. Multihoming is a mechanism for attaching an end system to two or more network access points without the need for a system setting up a call to it to be aware of the extra connectivity. In addition to enhancing survivability, this facility may be extended to support "mobile hosts" such as aircraft and ships.
(2)	Multi-endpoint connections [multi-addressing; multipeer data transmission (MPDT)].[82] In order to transmit data to a number of recipients, it is usually necessary to establish several connections and send separate copies of the data across each connection in turn. More efficient use is made of the communications resources if the sender has to transmit only one copy of the data. The network then takes care of routing, control, and distribution of the data.
(3)	Internetworking. Mechanisms are required to facilitate the interconnection of various NATO systems at the boundary point between subnetworks.
(4)	Network or system management functions. Management functions are required that may be of greater sophistication than those considered satisfactory for civilian networks. Management of broken networks in which layers of protocols are inoperable and fast responses to changes in network topology are essential to maintain important connections.
(5)	Security. Protection measures are required to prevent unauthorized access to information, preserve the integrity of data, and to mitigate against denial of service. [Note: Security includes access control, authentication, integrity, and confidentiality.]
(6)	Robustness (resilience) and quality of service. The range of quality of service parameters required for military systems exceeds that currently permitted within commercial OSI networks. In particular, in order to maximize the survivability of a network, the NATO aim is to maintain an adequate quality of service to the users (or at least to users operating above a given priority level) in the face of a severely damaged or partitioned network.
(7)	Precedence and preemption. In order to minimize congestion, particularly in a damaged network where resources are at a premium, it is desirable to be able to allocate resources on the basis of priority levels assigned to the connections being routed through the congested area. A facility is therefore required to associate a priority level with a connection when it is established.
(8)	Real-time and tactical communications. Certain applications are prepared to sacrifice such aspects of quality of service as sequencing and guaranteed delivery to achieve the minimum possible transit delay.

Source: *Use of OSI Standards in NATO—Strategic and Technical Issues*, Issue 2, TSGCE SG9, March 1988, NATO RESTRICTED.

A top-level view of how the eight military features identified above could potentially affect the layers of the OSI Reference Model is provided in Table 52. The entries in the table are based on the most recent editions of the draft OSI STANAGs (see Section 17.4).

81 The eight military features are listed in the *NATO Interoperability Planning Document* [Ref. NIPD 1993, Volume III] as specific military requirements/features that must be considered in development of standards.

82 As indicated in Section 9.2, work in ISO on MPDT has been suspended in SC21/WG1. The completed work is planned to be released as a Technical Report. Canada is serving as the point of contact within TSGCE SG9 for maintaining interest in MPDT in ISO. Canada has introduced a draft proposal in ISO on Multi-Party Communications that would address MPDT.

Table 52. Impact of Military Features on Layers of OSI Reference Model

Military Feature	OSI Layer 1	2	3	4	5	6	7
1. Multihomed, Mobile Host Systems			TBD				X
2. Multi-Endpoint Connection			X			TBD	X
3. Internetworking			TBD				
4. Network/System Management Functions	TBD	TBD	TBD	TBD			X
5. Security	X		X			TBD	X
6. Robustness and Quality of Service	TBD		X	TBD		TBD	TBD
7. Precedence and Preemption			X	TBD			X
8. Real-Time and Tactical Communications			TBD	TBD		TBD	TBD

Key: X = A deficiency has been identified in the applicable draft STANAG; TBD = "to be determined"; and blank = "not applicable."

Sources: *Use of OSI Standards in NATO-Strategic and Technical Issues*, Annex 6, *Summary of Impact of Military Feature on Layers of Reference Model*, TSGCE SG9, 1 March 1988, NATO UNCLASSIFIED; *Commentaries on the STANAGs of WG1*, Contribution by France to TSGCE SG9/WG1, February 1989, NATO UNCLASSIFIED; the *NATO OSI Security Architecture (NOSA)*, March 1988, NATO UNCLASSIFIED; and recently released draft OSI STANAGs (through December 1991).

17.3 Organizational Responsibilities—TSGCE Subgroup 9

Current SG9 Organization. TSGCE SG9 has the primary responsibility in NATO for reviewing the military requirements, identifying the potential impact on the OSI standards planned for use in each of the seven layers of the ISO and NATO Reference Model, defining the deficiencies and services required to address these requirements at each layer, and developing draft STANAGs that conform to the Reference Model and provide for the needed services. As a result of the 1991 TSGCE reorganization, SG9 has three permanent WGs, three ad hoc working groups (AHWGs), and one project group (PG) [Ref. TSGCE 1991b; Curcio 1994]:

- WG4 on Data Links—established in 1991 to consider future data lines and data link architectures. AHWGs have been formed under WG4 to deal with Data Link Interoperability and Data Link Testing.
- WG5 on OSI Layers 1-4—responsible for networking, with specific responsibility for transport and relay profiles.
- WG6 on Upper Layers and Pan-Layer Issues--responsible for such issues as security, network management, quality of service, conformance, naming and addressing; and for application profiles. Note: the work of the former AHWG on Network Management was completed in June 1993; any further activity on network management will be done by WG6.
- AHWG on Integrated Services Digital Network (ISDN), subordinate to WG5—developing STANAGs for using ISDN standards developed through ITU-TS.
- AHWG on Military Message Handling System (MMHS), subordinate to WG6—developing MMHS profiles, which are expected to be completed in 1994.
- AHWG on Security—responsible for providing security architecture/standards and guidance to other groups as agreed by the SG9 plenary.
- Project Group (PG) 9 on Multifunctional Information Distribution System (MIDS) Low Volume Terminal (LVT)—not a permanent WG; PG9 was disbanded at the end

of 1993, and a NATO Project Steering Committee was established under the terms of a memorandum of understanding (MOU).

TSGCE SG9 maintains liaison with many NATO bodies and agencies, including ADSIA, TSGCE SG11 (Tactical Communications), TSGCE PG6 (Tactical Communications Systems for the Land Combat Zone—Post 2000), NATO Industrial Advisory Group (NIAG) SG6 (Compatibility of Naval Data Handling Equipment), ATCCIS PWG, and Allied Tactical Communications Agency (ATCA). Liaison will be initiated with the newly formed TSGCE SG12 on Information Systems, together with its two subordinate groups: WG2 on Data Processing and Management and the AHWG on ATCCIS. (The work of SG11, PG6, and SG12 is discussed in Chapter 18.)

A concern about the current structure of SG9 is the level of participation by the nations. For example, during the period July 1992 through December 1993 only five nations (GE, NE, NO, UK, and US) participated in more than half of the six semiannual meetings of WG5, and only one of these meeting had as many as seven participating nations. Only six nations attended the October 1992 SG9 plenary, and only seven nations attended the May and October 1993 SG9 plenaries. Canada has greatly reduced its previously very active role due to limited resources (but is still very active in the AHWG on Security). Resource limitations may affect other nations in 1994 and 1995.[83] Another concern is the lack of substantive STANAGs to provide the basis of NATO cooperation for the use of OSI standards in military systems. Many of the OSI STANAGs (and all of those now ratified) are principally cover sheets for international civil standards, and this is true of several other STANAGs still in draft form. The new focus of SG9 on profiles appears more substantive, but it is not clear if any of the nations are prepared to mandate the use of the emerging profiles. The key to cost-effective implementation is in influencing vendor products, which has been primarily driven by regional and international civil consortia of vendors, governments, and users; it is not clear whether TSGCE recommendations and standards will influence the commercial products.

TSGCE Reorganization. In May 1993, in response to direction from its parent organization, the Conference of NATO Armaments Directors (CNAD) [Ref. Beard 1993], a new structure and organization for TSGCE has been proposed based on guidance provided by the NATO International Military Staff (IMS) [Ref. Klein 1993]. The CNAD is seeking to restructure, streamline, and make more effective the organization and working practices of its Main Groups (such as the TSGCE). The goal is to provide more effective contributions by the Main Groups to the process of collective armament planning. Each Main Group has been directed to revise its terms of reference (TOR), with organization based on the following elements [Ref. Klein 1993]:

- Main Group promotes cooperation and technology development, procurement, and standardization that may lead to future military equipment and systems
- Standing Groups (SG) of the Main Group that concentrate on information exchange and direct supervision and management of subordinate groups
- Ad Hoc Groups (AHGs), established initially for 2 years, which provide the basis for armaments cooperation under the Main Groups and which actively develop STANAGs in conduction with pursuing materiel standardization activities (some may be specially approved as open ended)

---

83 In its May 1993 plenary, TSGCE SG9 noted the reduction in participation in WGs 5 and 6; this issue was to be raised by the SG9 Chair at the next TSGCE plenary.

- Project Groups (PGs), which may be formed when a cooperative venture has been identified and when interested nations have agreed to commit resources to a joint effort.

The Chair of TSGCE has proposed the following standing groups for TSGCE as a Main Group [Ref. Gladman 1993]:

- Communications Systems Group formed from SG11 and part of SG9
- Information Systems Group formed from SG12 and part of SG9
- Combat Support Systems Group formed from SG4 and SG5.

These standing groups would be responsible for (1) organizing information exchange within their areas in order to promote cooperative equipment and systems development opportunities; (2) identifying possible opportunities for cooperative equipment or systems development; (3) establishing and managing temporary working groups to investigate such opportunities in more detail; (4) identifying standardization objectives within their areas for which the nations are prepared to find resources and funds; and (5) establishing working groups to develop such standards.

The following working group structure has been proposed [Ref. Gladman 1993]:

- Communications Systems Group
  - Tactical Communications (a combination of WGs in SG11)—should bring together national experts to decide where real cooperative possibilities exist
  - Fixed (Strategic) Communications (WG5 and AHWG on ISDN in SG9)
  - Satellite Communications Systems (WG8 of SG11)
  - Data Links (WG4 of SG9)
  - PG[84] on Tactical Communications Post 2000 (PG6)
  - PG on Communications System Network Interoperability (CNSI)
  - PG on Multifunctional Information Distribution System (MIDS) (PG9)
- Information Systems Group
  - Electronic Mail and Messaging (AHWG on MMHS in WG6 of SG9)
  - Distributed Information Systems (a combination of WGs in SG9; responsible to the TSGCE but with tasking link to the ISWG of the NACISC)–covers an area of technology (including information systems security) that is vital to C3 systems effectiveness and that should form a part of the TSGCE effort; while cooperating with other NATO agencies (e.g., NSA, ACCSA), the TSGCE will have a lead role in technical standardization; this working group would also be tasked by the ISWG
  - Information Systems Engineering (responsible to the ISWG of the NACISC but with a tasking link to the TSGCE)—covers systems and software engineering, including acquisition methods and approaches
  - PG on BICES
  - PG on Ada Programming Support (SWG on APSE)
- Combat Support Systems Group
  - Identification Systems (SG5)
  - Navigation Systems (SG4).

The Chair TSGCE observed in a commentary on existing groups [Ref. Gladman 1993] that (1) SG9 currently has an extensive number of working groups but very little in the way of real

84 The TSGCE Chair noted that the five proposed PGs are all currently working under multinational memoranda of understanding and report directly to the nations involved and not to the TSGCE [Ref. Gladman 1993].

cooperation in actual systems development; (2) the standards work has been of high quality but its exploitation by the nations has been limited and painfully slow; (3) its seems likely that many nations will not implement the standards being evolved and this should be a major concern to the TSGCE; and (4) the focus now needs to shift away from standards to cooperation on the programs for which such standards are needed.

Regarding SG11 on Communications Systems, the Chair TSGCE observed [Ref. Gladman 1993] that (1) SG11 has a wide range of activities in the land tactical communications area but it is difficult to discern any strategy or coherence in these efforts when viewed as a whole; and (2) in the satellite communications field, the nations are extensively involved in major discussions of possible cooperation in the next generation satellite communications systems *but entirely outside the TSGCE framework*.

The Chair TSGCE proposed that, when approved by the TSGCE, the new Standing Groups should be established immediately and that TORs and proposed working group recommendations be submitted to the second TSGCE meeting in 1994.

Other Concerns. A view of the TSGCE SG9 Chair on the long-term strategy for NATO standardization (based on the ODP five-view model) is provided in Section 18.9.1. A number of OSI issues of concern to NATO organizations and being addressed in TSGCE SG9 are discussed in Section 18.9.4 (on OSI) and Section 18.9.5 (on ISDN). The needs of various NATO initiatives for standards being addressed in TSGCE are identified in Sections 18.2 to 18.8.

17.3.1 NATO Reference Models, Transition Strategy, and NOSIP Strategy

17.3.1.1 NATO Reference Models

STANAG 4250, *NATO Reference Model for Open Systems Interconnection (NATO RM OSI)*, Edition 2, was last ratified and promulgated by the Military Agency for Standardization in August 1990 (MAS/212-EL/4250) as Part 1: *General Description*. A third edition has been developed [DS(CCC-ICP)(93)703, November 1993] but not yet distributed for ratification. One of the outstanding issues in 1993 was whether the name of STANAG 4250 should be changed to NATO Reference Model for Open Systems Information Interchange and its scope broadened to include a reference model for voice and video communications [e.g., Integrated Services Digital Network (ISDN)]. Agreement was *not* reached on this change in the October 1993 plenary of TSGCE SG9, so the development of a reference model to address ISDN and related services will be continued as a separate document.

The parts and status of STANAG 4250 are as follows:

- STANAG 4250-1 (Part 1): *General Description*, Edition 2 of STANAG 4250, MAS/212-EL/4250, August 1990 (ratified and promulgated) (cf. ISO 7498-2)
- STANAG 4250-1.3 (Part 1): *Basic Reference Model*, Edition 3 of STANAG 4250, Draft, DS(CCC-ICP)(93)703 (distributed for staffing), November 1993 (cf. ISO 7498-2)
- STANAG 4250-2 (Part 2): *Security*, December 1993, NATO SECRET (submitted for staffing, final editing, and translation prior to distribution for ratification) (cf. ISO 7498-2)
- STANAG 4250-3 (Part 3): *Naming and Addressing*, Draft, DS(CCC-ICP)(93)117 (distributed for staffing) and AC/302-D/647 (distributed for ratification), March 1993 (cf. ISO 7498-3) (as of 25 January 1994, ratified by four nations)

- STANAG 4250-4 (Part 4): *Management*, Draft, DS(CCC-ICP)(93)1129 (distributed for staffing) and AC/302-D/648 (distributed for ratification), 26 April 1993, NATO UNCLASSIFIED (cf. ISO 7498-4, 10040) (as of 25 January 1994, ratified by four nations).

Three additional documents have been drafted as a new part of STANAG 4250, but agreement to distribute these drafts has failed in each case.

- *Military Factors*, Draft (preliminary), 1992 (submitted as Part 5; cancelled May 1993)
- *NSP Guidelines*, Draft (preliminary), 1992 [submitted as Part 6; rejected by TSGCE SG9 plenary in December 1992 and cancelled in May 1993; when this document becomes stable (sometime in 1994), it will be subsumed into the *NOSIP Strategy*]
- *NATO-Adopted Civil Standards*, Draft (preliminary), October 1993 (submitted as Part 5; work suspended by action of TSGCE SG9 in October 1993).

17.3.1.2 NTIS Transition Strategy

A major project of TSGCE SG9, led by the German delegation, is the development and maintenance of the *NTIS Transition Strategy*. The current version is the 1991 or Sixth Edition; it is dated November 1991 [Ref. NATO 1991] and was accepted by SG9 in December 1991. This document provides recommendations for international commercial standards, primarily from ISO and ITU-TS, and intercept strategies (stacks of standards) that can be used by the nations as part of a transition strategy prior to the promulgation of OSI STANAGs.

As noted in the January 1992 release (Edition 3) of WP 25, the following emerging standards not addressed in the Fifth or Sixth Edition should be considered: ODP, TM, security protocols, X-Protocol (X-Windows), GKS, CGI, PHIGS, CGM, SQL, IRDS, and RPC.

17.3.1.3 NOSIP Strategy

The *NATO Open System Interconnection Profile (NOSIP) Strategy*, Draft, September 1993, has been developed and distributed to the nations by TSGCE SG9 for review comment [Ref. NATO 1993a] in order to facilitate the identification, specification, acceptance, and procurement of military communications and information systems based on the use of commercial off-the-self (COTS) products that use international civil standards. When endorsed by the Conference of NATO Armaments Directors (CNAD), which is the parent body of the TSGCE, the *NOSIP Strategy* will be a mandatory source of NATO Technical Interoperability Standards (NTIS) in support of the NATO Interoperability Management Plan (NIMP) and the NATO Interoperability Planning Document (NIPD). (The current CNAD-endorsed source for NTIS is the *NTIS Transition Strategy* [Ref. NATO 1991].) The *NOSIP Strategy* applies to the procurement and installation of all NATO communications and information systems that provide or support NTIS. It also applies to national systems and components that must interoperate with NATO systems and with each other. The *NOSIP Strategy* was developed to:

- Achieve interoperability
- Maximize the exploitation of COTS products
- Reduce the proliferation of non-standard systems.

NOSIP is intended to provide an overall framework for NATO communications that addresses the requirement to provide different types of communication services and to support different types of applications over a variety of network types. The current version of the NOSIP Strategy focuses on OSI- and ISDN-based communications; other subnetwork technologies will be

included in future versions of the document. The three objectives of the *NOSIP Strategy* are as follows:

(1) To state NATO policy on the use of standards for communications for interoperable systems within NATO

(2) To provide a framework for the development, management, and use of NTIS to achieve interoperability among NATO systems

(3) To provide direction to assist in the procurement and acceptance of interoperable NATO systems.

The *NOSIP Strategy* seeks to achieve these objectives by providing the following advice:

- Recommendations for a standardized internetworking communications architecture
- List of standardized profiles and other communications standards to be used by the NATO member forces
- Guidance on the use of interim and intercept standards
- Guidelines for improving interoperability among NATO systems
- Guidance for procurement agencies and officials on the selection and use of the NTIS.

Several principles provide the underpinning for the *NOSIP Strategy*. They are the following:

- Promoting, to the maximum extent possible, open systems civil profiles and COTS products
- Promoting adoption of military requirements into the civil sector standardization process
- Promoting the selection and use of applicable civil international profiles (NATO standardized profiles will be created only where existing civil profiles are inadequate)
- Rationalizing the required range of interconnection services within a common architecture
- Recommending a subset of available standards and profiles to increase the ability of NATO systems to interoperate
- Encouraging the adoption of NOSIP specifications as a mandatory part of the procurement policy of NATO member nations.

The scope of NOSIP includes most of what was formerly the *NTIS Transition Strategy*, but with greater attention to the NATO C3 environment, architectural requirements and issues, profiles (using ISO taxonomy), and procedural issues. Upon publication of the *NOSIP Strategy*, the *NTIS Transition Strategy* will be considered to be subsumed by the NOSIP. The *NOSIP Strategy* comprises five parts:

- Part I, *Overview*—discusses the NATO C3 Environment, which includes reference to the NATO C3 Architecture, the NATO Tactical Communications Architecture—Post 2000, and the eight military features
- Part II, *Architecture*—discusses the NATO Reference Model (which includes both the OSI Reference Model and the CCITT ISDN Reference Model), security,[85] naming and addressing, network and systems management, and profiles
- Part III, *NOSIP Standards*—specifies and discusses those standards that have been approved for NATO use as NTIS, summarizes the taxonomy of profiles being used

[85] STANAG 4250-2, *NATO OSI Security Architecture*, is still under development. The most recent draft is Version 4.0, *NATO OSI Reference Model*, Part 2: *Security*, 9 December 1993. See Section 11.2.3.2.

for NATO (adapted from the ISO taxonomy), and provides a 95-item list of base standards and profiles for OSI and ISDN interconnections

- Part IV, *Procedural Issues*—identifies procedures for naming and addressing, registration, testing, and configuration management (see Sections 9.1.2, 12.2, and 12.3)
- Part V, *Procurement Guidance*—relates the NOSIP Strategy to various GOSIPs, specifies applicability criteria, and provides recommendations for use of the document in procurements.

Details of the current recommendations of the *NOSIP Strategy* are provided in WP 25 in several ways. The list of base civil standards is identified in Appendixes D and E with special marks to show that a standard is included in NOSIP. In addition, Appendix I portrays the profiles provided in NOSIP.[86] Other documents cited in NOSIP, such as STANAG 4250 and the OSI STANAGs 4251-59 and 4261-66, are listed in Appendix H and discussed in detail in Appendix J.

17.3.2 WG4 Activities and Plans for Data Link Standards

17.3.2.1 WG4 Activities

The first meeting of SG9/WG4 on Data Links was held in June 1991; five nations (FR, GE, NO, UK, US) participated in the December 1991 meeting. WG4 was created within SG9 to address such data link topics as media-independent data link architecture (MIDLA), Multifunctional Information Distribution System (MIDS),[87] unmanned aerial vehicles (UAVs), stand-off surveillance, target, and acquisition (SOSTA) systems, and reconnaissance, surveillance, and target acquisition (RSTA) systems.

Germany is joining France and the United Kingdom in Phase 2 of MIDLA. When Phase 2 is completed, it is expected that MIDLA participants will provide a recommendation to the TSGCE that tasks be initiated to prepared necessary STANAGs.

The primary activity of WG4 has been the review and coordination of STANAG 4175 to bring it into line with the Joint Tactical Information Distribution System (JTIDS) terminal.

WG4 has been discussing interoperability testing efforts, principally among nations implementing JTIDS or MIDS. Interoperability testing issues are being addressed, in part, in the MIDS Interoperability Interface Working Group, subgroup of PG9 on MIDS-LVT. Interoperability testing is viewed as a national responsibility, since NATO funds cannot be used for international testing. Risk reduction testing will include use of facilities of the US Joint Interoperability Test Center (JITC) at Fort Huachuca, Arizona.

A classified memorandum on Data Link Requirements prepared by the NATO International Military Staff has been provided for review (October 1992); comments were provided prior to the January 1993 TSGCE plenary.

17.3.2.2 WG4 Work Plan

WG4 has accepted responsibility for the maintenance and configuration management of STANAG 4175 on MIDS; currently (December 1991) ratified by 10 nations, STANAG 4175 will

---

86 Many of the profiles specified by NOSIP are summarized in Appendix I.

87 MIDS is a NATO form of the Joint Information Distribution System (JTIDS) developed in the US. The initial implementation in NATO used the Interim JTIDS Message Standard (IJMS), which is not interoperable with JTIDS. While there are significant differences in hardware, the future message standard for MIDS (STANAG 4175) is essentially the same as the TADIL J used in JTIDS.

be promulgated shortly. WG4 will address other data link issues such as NATO Improved Link Eleven (NILE) and UAVs. There was specific interest in investigating solutions to the UAV data link requirements but no interest in discussion of MIDLA (see Section 17.5.1 for discussion of MIDLA and other topics originally proposed for Nunn Amendment funding). The tasking assigned to WG4 is summarized in Table 53. WG4 is currently focusing on issues relevant to the introduction of MIDS nationally and in NATO and what the group should do to assist in that process. [Ref. Ahern 1991]

Table 53. SG9 Tasking Instructions for WG4 on Data Links

• To sponsor and develop technical interoperability standards for data links; control required test and configuration management of data link standards; and promote their use to avoid unnecessary proliferation of application specification data link equipment and systems
• To plan, initiate, and coordinate development, testing, and implementation of interoperable data link equipment and systems
• To provide advice for the TSGCE on all matters related to data links
• To maintain configuration control of STANAG 4175 and collate implementation/transition plans for the introduction of the MIDS within the nations and NATO; monitor its implementation; and identify areas for cooperative activities with the aim of initiating such activities
• To explore the subject of media independent data link architecture based on a layered structure
• To explore the use of an existing or initiate the development of a technical interoperability standard for a common data link for UAVs, SOSTA, and RSTA.

Source: *WG4 on Data Links Report to the Chairman of SG9*, AC/302(SG/9)D/96, Chairman WG4, December 1991, NATO UNCLASSIFIED.

17.3.3 WG5 Activities and Plans for Networking Standards[88]

17.3.3.1 WG5 Activities

The following activities have been reported by participants in SG9/WG5:

- In lieu of any further work on layer STANAGs, working on profiles to meet NATO requirements.
- Revising the draft STANAG 4250-1 to include the ISDN Reference Model as well as the OSI Reference Model.
- Working with WG6 to revise the *NSP Guidelines Document* (planned to become STANAG 4250-6). This document is viewed in SG5 as "a basis for the lowest common denominator of interoperability." In 1992 SG9 rejected including this document as Part 6, in part because of the strong resistance by application profile developers on the use of these guidelines (it was seen as not broad enough to accommodate WG6 profiles as well as profiles not based on the OSI Reference Model). The primary concern is with the base document, ISO/TR 10000, which prescribes a format different from that endorsed by EWOS. If current work in ISO to incorporate the EWOS format is successful, most of the concerns with the NSP Guidelines Document will be resolved. The *NSP Guidelines Document* was updated in October 1993 and sent to SG9 for approval. Once approved, it will be subsumed in the *NOSIP Strategy*. [Ref. Curcio 1994]
- Submitted (May 1993) four lower layer STANAGs to IMS for ratification when translation is complete: 4251, 4252, 4261, and 4262.

---

88 This section is based on the following sources: [Onufer 1992a], [Onufer 1992b], [Messina 1993a], [Messina 1993b], [Messina 1993c], and [Messina 1993d].

- Distributed (May 1993) two lower layer STANAGs for editing and agreement: 4253 and 4254. Requested that STANAGs 4253 and 4254 be finalized and forwarded to the SG9 secretary for ratification.
- Distributed a multi-part draft STANAG for TC1111(M) and TC1121(M), which describe permanent access to a packet-switched data network using the COTS and CONS. [Ref. Curcio 1994]
- Preparing ISDN STANAGs for final comment preceding ratification: 4459, 4460, 4461, 4462, and 4463.
- Preparing NSP STANAGs for final comment preceding ratification: 4407, 4408, and 4409. STANAGs 4408 and 4409 have been distributed for ratification.
- WG5 has recognized the importance of a LAN-to-ISDN interface to support the NATO C3 Architecture. STC submitted a proposal in 1992 for a RA5n.4nnn(M) profile to address this requirement, and agreed to produce a draft RA5n.421n profile. This profile would make use of ES-to-IS routing, IS-to-IS routing, and the Inter-Domain Routing Protocol in the Network Layer to support the connectionless network protocol. This work appears in draft STANAG 4413.
- Evaluating and preparing comments on draft STANAG 4250-7 (formerly planned as an annex to 4250-1) on *NATO-Adopted Civil Standards*, with the recommendation that standards cited in this document requires no further work in SG9.
- Commenting on document produced by SG9 secretariat on data links.
- Addressing multicast service, which is designed to provide more efficient transmission of identical data to two or more destinations, primarily to conserve bandwidth and possibly reduce delays in transmission. [The US provided WG5 the status of US proposals in ISO to extend the connection-oriented transport protocol (ISO 8473) to incorporate reliable multicast services.] [Ref. Curcio 1994]

17.3.3.2 WG5 Work Plan

The current draft work plan for WG5 identifies the following activities for 1994 [Ref. Onufer 1993]:

- NOSIP
  - Manage lower layer standards status
  - NSP Guidelines in NOSIP
  - Extensions to ISO taxonomy of profiles
- NATO and national networks
  - Identify interoperability requirement (e.g., MC 277)
  - Make recommendations on NATO Networking Architecture
- Profiles
  - Relay ISDN-LAN 9 (to be completed April 1995)
  - Relay X.25-LAN (TBD)
  - Subnetwork-related profiles (TBD)
- Security
  - Implementation in profiles (TBD)
- Base standards
  - CO protocols (routing, subnetwork independent) (TBD)
  - Revision of 8473, including SNIP (under development; completion October 1994)
  - Multicasting (under development; completion April 1995)

- Management
  - Produce managed object definitions for military enhancement (under development; completion October 1994)
- ISDN
  - Prepare tasking for the AHWG on ISDN, approve the work plan, and approve output documents (ongoing)
- Liaison with WG6, SG11 (WG1), CNSI project, SG9 AHWGs, PG6, and NIAG SG6 (ongoing).

17.3.3.3 Areas Not Yet Addressed in WG5 Work Plan

NACISA has promulgated a policy statement that makes the use of CLNP and TP4 mandatory for all NATO infrastructure programs. This is of concern to members of WG5 (e.g., UK delegation) who are interested in the use of CONS. WG5 was requested to support the development of subnetwork independent CONS protocols and associated routing protocol standards, as well as working on CLNS standards development. [Ref. Messina 1993b]

Another proposal for new work (not yet incorporated into the 18-month work plan) is a LAN-to-X.25 relay. Neither NACISA nor Canada, who agreed in 1992 to investigate availability of resources for this work, have found resources to lead such an effort. [Ref. Messina 1993a]

17.3.4 WG6 Activities and Plans for Upper Layers and Pan-Layer Issues

17.3.4.1 WG6 Activities

The following activities have been reported by SG9/WG6 participants.

- Preparing STANAGs for final comment preceding ratification: 4406 (message handling) and 4407 (systems management).
- Submitted (May 1993) STANAG 4250-3, Naming and Addressing, in final form for ratification (Ratification is underway and has received US concurrence.) [Ref. Curcio 1994]
- Submitted (May 1993) two upper layer STANAGs to IMS for ratification when translation is complete: 4257 and 4267.
- Developing a registration document on Message Handling names, Directory names, and managed objects.
- Work on upper layer security. Continuing liaison with the AHWG on Security to seek near-term solutions for authentication and non-repudiation with regard to Directory service. One solution is the use of asymmetric encryption tables.

17.3.4.2 WG6 Work on MMHS

The AHWG on MMHS continues liaison with developers of Allied Communications Publication (ACP) 123 and harmonization with STANAG 4406. A separate annex (Annex D) of STANAG 4406 specifies the ACP 127 gateway (no provision has yet been made for an ACP 123 gateway).

MMHS will be addressed in a separate Application Layer standard, STANAG 4406 [Ref. STANAG 4406 1991] (September 1991; see Section 17.4.2). STANAG 4406 will incorporate four elements that are being developed simultaneously by the AHWG on MMHS: Base Standard, Rationale, an Alpha Profile, and a Beta Profile. The Alpha profile is intended to address strategic and tactical applications where bandwidth limitations are not severe, and the Beta Profile is intended to address tactical applications where bandwidth is severely limited. For the Beta profile, the AHWG on MMHS assumes that bandwidth will be conserved by eliminating all but the most

vital services of MHS. These profiles are being written as a "delta" or change to the MHS profile being developed by the European Workshop for Open Systems (EWOS) [Ref. EWOS 1990a]. Each MMHS profile will be included in STANAG 4406 as a separately ratifiable annex. [Ref. SG9/WG1 1990c]

The AHWG-MMHS work has been separated into two sets of functional groups. The first set consist of military messaging services, notification, security, redirection, distribution lists, conversion, ACP 127, and MMHS gateways. The second set will provide directories, current draft of STANAG 4406 addresses the first set of functional groups. [Ref. Krick 1991]

The *Intercept Profile for MMHS*, based on MHS:1984, has been amended (Issue 2) to include full support for ACP 127 [Ref. MMHS 1990]. It was completed in February 1990. Issue 2 has a new annex (Annex C) on implementation options for the military header extensions. Issue 1 of the profile was accepted as an intercept strategy for the *NTIS Transition Strategy* [Ref. NATO 1991]; however, depending on choices of interoperability parameters, MMHS implementations based on MHS:1988 may not be backwards compatible with MHS:1984 implementations. Only MHS:1988 is in the *NOSIP Strategy*.

One area of MMHS not addressed by MHS:1988 is support for trusted functionality. Such support may be covered by the NLSP, TLSP, and TCS to carry out services associated with trusted functionality. The May 1989 meeting of the AHWG-MMHS was devoted to security and succeeded in developing two functional groups of security services. One of these does not require use of asymmetric encipherment mechanisms, but precludes direct support of non-repudiation services. These have both been accepted by EWOS. The AHWG-MMHS sought guidance from the AHWG on Security to identify suitable encipherment mechanisms to support these services. [Ref. SG9/WG2 1989] The AHWG on Security confirmed the need for asymmetric cryptographic mechanisms and indicates that such mechanisms need to be offered by the Nations for consideration and approval by the appropriate NATO authorities. [Ref. AHWG-S 1990a]

17.3.5 AHWG on Security[89]

17.3.5.1 Activities of AHWG on Security

The AHWG on Security has been working almost exclusively on developing a security protocol for the Network Layer of the OSI Reference Model. The goal was to define a security protocol specification and service definition that would be a subset of whatever was adopted as an international standard. This effort was labeled the Trusted Communications Sublayer (TCS).

With input from representatives of the AHWG on Security, the JTC1/SC6/WG4 combined three security protocols into the Network Layer Security Protocol (NLSP). They were the US SDNS SP3, Northern Telecom's SPX, and the UK's End-to-End Security Protocol (EESP). NLSP reached IS status at the September 1993 meeting of SC6 in Seoul (ISO/IEC 11577, October 1993).

Final editing of the *TCS Protocol Specification and Service Definition* by the AHWG on Security will make it possible to describe the TCS as a profile of ISO/IEC 11577 (NLSP) with some local procedure extensions. These local procedure extensions to NLSP are only necessary in the connection-oriented mode of operation, since there are no fundamental differences between the TCS and NLSP in the connectionless mode of operation.

---

89 Based on the following sources: [Staton 1994], [McLane 1993a], and [McLane 1993b].

The AHWG on Security has developed three major references for use in SG9: *NATO OSI Security Architecture (NOSA)* [Ref. NOSA 1988], *Security Architecture for NATO Information Systems Interconnection (SANISI)* [Ref. SANISI 1989], and the *NATO Network Security Information Classification Guideline*. NOSA was developed as an unclassified document to give guidance to contractors and procurement managers on the preferred placement of security services within OSI conformant systems. SANISI provided more detailed rationale on the placement of security services and mechanisms with the OSI Reference Model. A key element of both NOSA and SANISI was the requirement for a TCS security service at Layer 3. No security services were identified for Layer 4, the Transport Layer. The final NOSA document is Version 3.1, dated September 1988, and the final SANISI document is Version 2.0, dated April 1989. Additional documents to support the TCS are the *TCS Applications Guidelines* that define the placement and operation of the TCS within both connectionless and connection-oriented modes of operation, the *TCS Service Definition* (Annex B of STANAG 4253), and the *TCS Protocol Specification* (Annex B of STANAG 4263). These documents are expected to become stable in early 1994.

Work has begun on Part 2 (*Security*) of STANAG 4250 to make it the appropriate reference document incorporating the pertinent parts of SANISI and NOSA. The NATO security architecture for voice and video communications is currently under development and is expected to be included in a supplement to this STANAG.

17.3.5.2 Work Plan of AHWG on Security

The 18-month work plan is being revised by the AHWG on Security; it will address the deliverable documents related to the TCS, management, and upper layer issues. Table 54 identifies the specific tasks given to the AHWG on Security in the revised special tasking instructions.

Table 54. Planned Activities for AHWG on Security

(1)	Develop and maintain a network information security classification guideline for use by NATO elements when developing network protocols and architectures
(2)	Develop and refine a security architecture for NATO information systems based on the OSI Reference Model
(3)	Define the security services required for NATO military application and determine the placement within the basic reference model
(4)	Influence ISO/ITU-TS and other standards bodies to adopt additional security services as appropriate
(5)	Develop NATO STANAGs for the security architecture and communications protocols based on existing standards
(6)	Extend applicable communications standards to accommodate military security services where necessary
(7)	Complete the detailed design work on security layers and sublayers leading to protocol specification, service definitions, and user requirements documents
(8)	Review, advise, and recommend security annexes to all layer STANAGs
(9)	Liaise with other NATO groups, both inside and outside SG9, working on network security issues.

Source: *Special Report to the TSGCE by the Chairman SG9*, Annex XIII, *Special Tasking Instructions for the Ad Hoc Working Group on Security*, AC/302-D/602, July 1991, NATO UNCLASSIFIED.

17.3.6 AHWG on ISDN[90]

An AHWG on ISDN was formed by TSGCE SG9 in 1989 to review the status of ISDN and the applicability of these standards to NATO. An overview of the eight military features was adopted at the April 1990 meeting; the results are given in Table 55 (note that the suitability of the ISDN protocols for use in the tactical domain was agreed to be outside the scope of the meeting). [Ref. AHWG-ISDN 1990]

90 Based on the following sources: [McLane 1993a], [McLane 1993b].

Table 55. Military Features for ISDN

(1)	Mobile Hosts and Multihomed Systems. A number of scenarios are being discussed, some outside the ISDN domain (e.g., in the tactical area) and some within the strategic ISDN domain (e.g., as user moving from one PABX to another). Only strategic ISDN domain issues are currently being addressed in the AHWG on ISDN. It was agreed that ISDN Suspend/Resume procedures for moving during a call were not applicable to mobile hosts. Some form of slow mobility is required where a user may, for example, move between extensions on the same access switch or even to a different access switch and still maintain the same user identity. This would require a type of registration and cancellation procedure where a user takes the user identity around a fixed network. Specific NATO procedures may be required to realize this feature—further study is required. Procedures associated with the cellular radio service are issues mainly applicable to the tactical domain.
(2)	Multi-Endpoint Connections. Information needs to be multicast (or broadcast) to several destinations. A central issue is whether a unidirectional service was required for this feature: (a) If the requirement were defined in terms of a conference call (bidirectional), then commercial products are expected to be available. (b) If broadcast facilities were provided at the Application Layer using packet procedures, no specific NATO procedures are required. (c) If broadcasting were required on all bearer services (e.g., voice and data), then the AHWG on ISDN should wait for ITU-TS/ETSI to define this feature. It was generally agreed that the multi-endpoint feature is for data application rather than voice; further study is required on the requirement for voice.
(3)	Internetworking. The *NATO C3 Architecture* (Volume 4, *Communications Subsystem*) allows both the "T" reference point and the K, M, and N reference points as possibilities for internetworking. If the "T" reference point were chosen, then a number of enhancements would be required for NATO, such as satellite and routing indicators.
(4)	Network and System Management. ITU-TS is defining a network management structure in both the user-network area (Q.940) and within the network. This work is at the architectural level and has not resulted in a definition of detailed procedures. Of particular interest to SG9 are the management functions of Section 3 of Q.940 for fault, configuration, accounting, performance, and security management—all aligned with OSI management functions. In addition, management reference models have been defined.
(5)	Security. Key issues are the applicability of the TCS to ISDN (for data services), the impact of ISDN on the security services defined in STANAG 4250-2 (Part 2): *Security*, and the definition of new security features using ISDN capabilities (e.g., common channel signaling).
(6)	Robustness and Quality of Service. The only possible special NATO requirement identified is the QoS parameter, should the ISDN network performance figures given in I.350 not prove to be adequate for military applications.
(7)	Precedence and Preemption. This feature is already being addressed (service definition and information).
(8)	Real-Time and Tactical Communications. No special real-time requirements are foreseen for ISDN. Note that the discussion was limited to interworking with a tactical network and to the concept of a strategic ISDN activity either as a transit network or to gain access to an ISDN user.

Source: *Report of the 2nd Ad Hoc Meeting on ISDN in Paris, April 1990*, TSGCE SG9 AHWG on ISDN, May 1990, NATO UNCLASSIFIED.

Note: The suitability of the ISDN protocols for use in the tactical domain was agreed to be outside the scope of the assessment leading to these requirements.

One of the issues for discussion within the AHWG on ISDN has been the alternative facsimile (FAX) standards for ISDN: G3 (64 kbps) versus G4.

17.3.7 PG9 on MIDS LVT

PG9 on the MIDS Low Volume Terminal (LVT) was formed by TSGCE to develop an MOU for an multinational, multi-Service, cooperative program for a light-weight tactical information distribution system. (PG9 was disbanded at the end of 1992, and a NATO Project Steering Committee was established under the terms of an MOU.)

The LVT would be a pre-planned product improvement to the Joint Tactical Information Distribution System (JTIDS) that would reduce the size (from 1.7 to 0.6 cu ft) and weight (from 135 lb to 65 lb). The LVT would reuse the JTIDS software, including the LINK 16 (JTIDS)

standard (and not IJMS). The participating nations[91] (FR, SP, IT, GE, and US) plan ground-based, airborne, and ship-based employment (the US would use it for the F/A-18s). The project definition phase (1987-1990) was followed by the pre-engineering and manufacturing development (EMD) phase (1991-1992), in which the request for proposal (RFP) was finalized and released, proposals evaluated, and contracts negotiated. National contractors are expected to be awarded work at the same proportion as national funding. The EMD phase (1992-1997) began with contract award and includes design, fabrication, integration, test, and technical data package verification. The production phase (1997-2010) is initially planned to acquire 2,750 LVTs (plus spares). [Ref. TSGCE 1991g]

17.4 Status of NATO Open System STANAGs

17.4.1 OSI Layer STANAGs

Table 56 identifies the STANAGs being developed that will specify ISO standards and applicable military options and extensions, if any. Work has begun on all these STANAGs, but only the NATO Reference Model, STANAG 4250, has been ratified. Originally, TSGCE SG9 planned to issue a single STANAG for all services and a second STANAG for all protocols at each layer, giving a total of 14 STANAGs in addition to STANAG 4250, the NATO Reference Model. In October 1987, TSGCE SG9 agreed [Ref. UK 1988, Annex 1.2] to work at the Application Layer for single STANAGs for each Application Layer service, such as MMHS (STANAG 4406). Protocol specifications as well as service definitions would be addressed in that STANAG.

Little progress on the lower layer STANAGs has been made during the past 2 years. Most of the changes observed on the various drafts of these documents during this period have been editorial. In a few cases, some PICS proformas have been added. Since these documents, for the most part, adopt international standards without enhancements, it is not clear why these standards were not released for ratification in 1991. The need for the layer STANAGs is not clear, especially if their primary role is to provide cover sheets for international civil standards.

17.4.2 Application and Multi-Layer STANAGs

The only Application Layer STANAG that has been produced in draft form is the draft MMHS STANAG 4406. The parts of this standard are as follows:

- Annex A—MMHS Extensions to ISO 10021 Series, Draft
- Annex B—Security Aspects of MMHS (under development)
- Annex C—Alpha Profile Set (a delta specification to EWOS profiles): AMH1x(M) on Common Facilities and AMH9x(M) on Military Messaging, Draft
- Annex D—Alpha/ACP 127 Gateway (under development)
- Annex E—Alpha/MMHS(84) Gateway (under development)
- Annex F—Alpha/MHS(88) Gateway (under development)
- Annex G—Beta Profile Set (under development)
- Annex H—Beta/ACP 127 Gateway (under development)
- Annex I—Beta/Alpha Gateway (under development).

---

91 Norway, Canada, and the United Kingdom participated in the project definition phase but declined to continue into development and procurement.

Table 56. NATO OSI Standards

Relation to OSI	Service Definitions			Protocol Specifications		
	STANAG	Status	Doc. Date	STANAG	Status	Doc. Date
Reference Model	4250, 4250-1	Ratified	21 August 1990		N/A	
	4250-2	Staffing	December 1993		N/A	
	4250-3	Draft	21 March 1993		N/A	
	4250-4	Draft	26 April 1993		N/A	
	4250-5X	Cancelled	1992		N/A	
	4250-6X	Cancelled	1992		N/A	
	4250-5Y	Cancelled	October 1993		N/A	
Layer 1	4251	Staffing	30 April 1993	4261	Staffing	17 March 1993
Layer 2	4252	Staffing	26 March 1993	4262	Staffing	18 March 1993
Layer 3	4253	Draft	18 March 1993	4263	Draft	19 March 1993
Layer 4	4254	Staffing	19 March 1993	4264	Staffing	19 March 1993
Layer 5	4255	Ratified	22 January 1993	4265	Ratified	22 January 1993
Layer 6	4256	Ratified	22 January 1993	4266	Ratified	22 January 1993
	4258 (ASN.1)	Ratified	22 January 1993	4259 (ASN.1 BER)	Ratified	22 January 1993
Layer 7	4257	Staffing	November 1993	4267	Staffing	November 1993
Layer 7	4406 (MMHS)	Draft	November 1993		N/A	
Profile	4407 (Mgmt)	Draft	15 May 1993		N/A	
Profile	4408 (COTS/CLNS))	Draft	October 1993		N/A	
Profile	4409 (COTS/CLNS))	Draft	7 April 1993		N/A	
Profile	4410 (CLTS/CLNS))	Draft	7 April 1993		N/A	
Profile	4413 (CLTS/CLNS))	Draft	January 1993		N/A	

Note: Staffing means that a final draft has been submitted by Subgroup 9 to the NATO International Military Staff for translation and distribution to the nations for ratification.
Source: [Rannestad 1994].

The initial draft STANAG 4406 will be circulated for ratification with the Military Base Standard (Annex A) and the ALPHA Profile Set (Annex C). Annex A provides the set of extensions to civilian message handling systems for Interpersonal Messaging Service (IPMS) required for military messaging. Annex A is also known as the Military Base Standard.

Table 57 identifies the military features as they affect MMHS. Previous editions of the MMHS draft STANAG have included additional material on *Scenarios and Rationale*, which provided detailed specification of the scenario of application, rationales behind the major decisions, and discussion of the support of the subset of the eight military features that are applicable to a store-and-forward messaging environment. This document is now being prepared separately. The intent is to have an excerpt from this document included in the 1991 edition of the MMHS STANAG, but this has not yet been done. [Ref. TSGCE 1991h]

Table 57. Status of X.400(MHS)-1988 Relative to the Eight Military Features

(1) Multihomed/Mobile Host

(a) Multihoming applies to MMHS applications in two ways: multihoming User Agents (UAs) and multihoming MTAs. In the first case, the MHS must allow a single user to have more than one Originator/Recipient (O/R) name. The second case requires MTAs that answer to more than one name. In both cases, the capability in question is outside the scope of the communications standards, but is permitted as an implementation option. Capabilities for multihoming would have no direct impact on either MHS services or protocols, but are instead more focused on the lower layers.

(b) Similarly, mobile hosting can also be applied to either the MTA or UA. In either case, the key requirement to support mobile hosting is the capability for the functional object in question to disconnect from the network for a period of time without serious consequence. In MMHS there are two mechanisms to support mobile hosting of the UA. One such mechanism is the use of a message store (MS) to act on the UA's behalf while the UA is off line. The second mechanism is use of the Hold for Delivery element of service, in which the service element instructs the MTS to defer delivery of a UA's messages until a later time. No such mechanisms are available to the MTA, however.

(2) Multipeer Data Transmission (MPDT)

Since MHS applications are store and forward (i.e., connectionless) in nature, no end-to-end connections are provided or required by MMHS. However, the MMHS does provide a connectionless MPDT capability in the form of multi-addressed messages. This feature allows a single message to be sent to several recipients with a single submission to the MTS. The MTS is then responsible for performing traffic splitting at the appropriate time. Note that traffic splitting could be substantially more efficient if supported by a lower layer MPDT function

(3) Internetworking

Internetworking is addressed by the provision of MMHS/ACP 127 and MMHS/civilian gateway definitions. Gateways could also be created to other systems that perform similar message handling functions, but such gateways are at present beyond the scope of MMHS.

(4) Network and System Management

Network management is a pan-layer issue that falls under the auspices of the AHWG-OM in SG9. The AHWG-MMHS will continue to identify MHS-related topics to be considered by AHWG-OM.

(5) Security

Security is a pan-layer issue that falls under the auspices of the AHWG on Security in SG9. The AHWG-MMHS will continue to identify MHS-related topics to be considered by the Security AHWG.

(6) Robustness and Quality of Service (QoS)

Most aspects normally associated with robustness and QoS have no meaning in the Application Layer. Three MHS characteristics have been identified as significant in terms of robustness and QoS: loss of messages, end-to-end delivery time requirements, and selection of security services. QoS aspects relating to link quality, hop-by-hop transmission delay, and throughput are primarily lower layer issues, and in any case have little meaning for a store-and-forward Application Layer process.

(a) Loss of message is addressed by the MMHS expansion of X.400's redirection capability. This provides a dead letter box at each MTA so that messages will always be delivered rather than discarded. MMHS also provides both delivery and nondelivery receipt capability to provide additional assurance of delivery.

(b) MMHS has specified end-to-end delivery time requirements consistent with those used by ACP 127. The hop-by-hop transmission delay and throughput necessary to achieve those end-to-end times are lower layer issues.

(c) Selection of appropriate security services is largely dependent on the security policy in force. This policy will determine what services will be enabled during the origination of a message based on its classification or other factors. This selection could be done either technically or procedurally, however, and thus is purely an implementation issue. Whatever solution is used will impact only the originator and will not require changes to the communication protocols.

(7) Precedence and Preemption

The established requirement for military priority in message handling is four levels based on ACP 127. The MMHS base standard provides six priority levels in all protocols necessary to support the use of precedence and preemption in any implementation. However, it is the intent of the AHWG-MMHS to develop functional profiles that support six levels of priority in the UA-to-UA protocols but only three levels in the corresponding MTA-to-MTA protocols. Use of these provided information elements to support precedence and preemption in either the UA or MTA is an implementation issue.

(8) Tactical and Real-Time Communications

MMHS has specified end-to-end delivery time requirements that are purported to represent the tactical environment. In addition, the AHWG-MMHS plans the development of a *Beta Profile* tailored to low bandwidth tactical applications.

Source: *Draft STANAG on Military Message Handling System*, February 1990, NATO UNCLASSIFIED.

17.4.3 NATO Standardized Profile (NSP) STANAGs

The work of TSGCE SG9 in 1993 has focused on development of NATO Standardized Profiles (NSPs). Table 58 identifies the drafts under development.

Table 58. Status of NATO Standardized Profiles

STANAG 4408, NATO Standardized Profile - Connection-mode Transport Service over Connectionless-mode Network Service, Draft (in final editing prior to translation for ratification), October 1993, NATO UNCLASSIFIED
- Part 1: Subnetwork Type Independent Requirements for Group TA, Preliminary Draft (cf. ISO 10608-1)
- Part 2: TA5n(M) Subnetwork Type Dependent, Media Independent Requirements for LANs, Preliminary Draft (cf. ISO 10608-2)
- Part 3: TA51(M) Subnetwork Type Dependent, Media Independent Requirements for CSMA/CD LANs, Preliminary Draft (cf. ISO 10608-2)
- Part 4: TA54(M) Subnetwork Type Dependent, Media Independent Requirements for FDDI LANs, Preliminary Draft (cf. ISO 10608-6)
STANAG 4409, NATO Standardized Profile - Connection-mode Transport Service over Connection-mode Network Service (Military), Draft (in final editing prior to translation for ratification), 7 April 1993, NATO UNCLASSIFIED
- Part 1: Definition of Profiles TC1111(M)/TC1121(M), Preliminary Draft (cf. ISO 10609-6)
- Part 2: Subnetwork Type Independent Requirements for Group TC, Preliminary Draft (cf. ISO 10609-2)
- Part 3: TA51(M) Subnetwork Type Dependent Requirements for Permanent Access to a Packet Data Network Using Virtual Call, Preliminary Draft (cf. ISO 10609-9)
STANAG 4410, NATO Standardized Profile - Connectionless-mode Transport Service over Connectionless-mode Network Service, Draft, 7 April 1993, NATO UNCLASSIFIED
- Part 1: Subnetwork Type Independent Requirements for Group UA, Preliminary Draft
STANAG 4413, NATO Standardized Profile - Relaying the Connectionless-mode Network Service
- Part 1: Subnetwork Type Independent Requirements for Group RA, Edition 2, January 1993 (cf. ISO 10613-1) (under development)
- Part 2: Subnetwork Type Dependent, Media Independent Requirements for LANs, Edition 2, January 1993 (cf. ISO 10613-2) (under development)
- Part 3: ISDN Subnetwork Dependent, Media Dependent Requirements for Circuit Switched B-Channel Operation, Edition 2, January 1993 (under development)
- Part 4: Profile RA51.4212, Edition 2, January 1993 (under development)

17.4.4 ISDN STANAGs

The following draft STANAGs are being developed for ISDN services:

- STANAG 4459, *ISDN Bearer Services*, Draft (in final approval prior to submission for translation and ratification), 11 May 1993 (cf. I.230)
- STANAG 4460, *Layer 1 Specifications for ISDN Basic Rate Access at the S/T Reference Point*, Draft (in final approval prior to submission for translation and ratification), 11 May 1993
- STANAG 4461, *Layer 1 Specifications for ISDN Primary Rate Access at the S/T Reference Point*, Draft (in final approval prior to submission for translation and ratification), 11 May 1993
- STANAG 4462, *Layer 2 Specifications for ISDN Basic and Primary Rate Access at the S/T Reference Point*, Draft (in final approval prior to submission for translation and ratification), 11 May 1993
- STANAG 4463, *Layer 3 User to Network Call Control*, Preliminary Draft, 8 April 1993
- STANAG 4464, *Signalling System No. 7 Message Transfer Part (MTP)* (under development)

- STANAG 4465, *Signalling System No. 7 ISDN User Part (ISUP)* (under development)
- STANAG 4466, *ISDN Teleservices* (under development)
- STANAG 4467, *ISDN Supplementary Services* (under development)
- STANAG 4468, *QSIG* (under development).

17.5 Development of Other Technical STANAGs

This section identifies non-OSI STANAGs that appear to be relevant to information systems. Media-dependent STANAGs (e.g., tactical data links) are not addressed.

17.5.1 Media-Independent Data Link Architecture (MIDLA)

MIDLA was suggested to TSGCE by ADSIA in 1986 [Ref. ADSIA 1986]. During the period 1987-1989, the Nations attempted to identify Nunn Initiative funding for MIDLA, but these efforts were unsuccessful. At the October 1989 SG9 plenary meeting [Ref. TSGCE 1989], the Nations agreed that development of a data link architecture based on the OSI Reference Model to replace antiquated data links was extremely important. However, it was also agreed that resources were not available within SG9 to address the breadth, complexity, and technical aspects of that subject. SG9 agreed to send a letter to TSGCE stating the importance and magnitude of this project. In addition, the Nations were asked to reassess the availability of resources relative to the MIDLA project.

MIDLA is one of the topics suggested for discussion in the newly created WG4 on Data Links. However, it is not an item of current interest to that group (see Section 17.3.2). A bilateral agreement has been established between France and the United Kingdom regarding future data link architectures. At the September 1991 meeting of WG4, France indicated that MIDLA development has not progressed sufficiently for it to be brought into the SG9 forum. [Ref. Ahern 1991]

Further, ADSIA has received an STC study, *An Architecture Based on OSI Principles for NATO Tactical Data Links* [Ref. SHAPE 1989], and has indicated to TSGCE SG9 that no further work on behalf of ADSIA is required for MIDLA. [Ref. ADSIA 1990] However, tactical data link architecture is being addressed by the TSGCE AHWG on Restructuring as a potential area of work. SG9 has indicated that if the SG9 terms of reference are amended to include tactical links, guidance from the TSGCE would be required on providing necessary resources. [Ref. TSGCE 1990k, TSGCE 1990b]

17.5.2 Network Independent Interface (NIIF)

NIAG SG6 is developing a draft specification of a Network Independent Interface (NIIF). This was briefed to the TSGCE SG9 AHWG-OM in February 1989. NIIF is a concept for a combat system data distribution interface that could be used by the NATO Frigate Replacement for the 1990s (NFR90), a program currently in a project definition phase.

In a subsequent joint meeting with the NIAG SG6 and TSGCE SG9/WG1 in June 1989 [Ref. NIIF 1989], the NIIF was identified as a project to (1) put NACISA in the lead to resolve interface problems and provide management structure for such projects; (2) provide near- and mid-term standards specification for ACCIS interoperability; (3) initially develop interface specifications to pass character-oriented messages between existing systems; and (4) evolve the specification so that it will be suitable for other services (e.g., file transfer, virtual terminal). The specifications were to be based on ISO OSI standards and on functional profiles of SPAG and CEN/CENELEC that are adopted in the *NTIS Transition Strategy*: T.21 Permanent Circuit (telephonic), T.22

Switched Circuit (telephonic), and T.31 Permanent Access to a PSDN. BID-1000 and KG-84 were identified for communications security. The message handling area was based on A/3211 from the EWOS.

As early as September 1987, NIAG SG6 proposed a draft STANAG for *NATO Naval Intra-Ship Tactical Control and Data Handling Open Systems Interconnection, Network Independent Interface, Transport Service Definition for Connection-Mode Transmission.* [Ref. NATO 1987a] This proposal was based on ISO 8072 with "additions and deletions, where necessary, to reflect a unique Naval, intraship, interpretation to it." The NIIF is identified in this proposal as a collection of standards that provide the complete definition of an interface between the User and the Data Transfer System, based on unique requirements for real-time, fault tolerant information exchange between peer systems.

17.5.3 Lightweight Protocols

The TSGCE AHWG on Restructuring has noted that the work of NIAG SG6 is closely related to the work of TSGCE SG9 on OSI standards. Both groups are interested in the area of lightweight LAN profiles for multi-Service use. The basis for the intraship LAN profile being developed by NIAG SG6 is based on France's GAM-T-103, as is the US SAFENET profile and the more general Xpress Transfer Protocol (XTP) profiles. [Ref. AHWG-OM 1990]

The XTP is a lightweight (providing simplicity and low overhead) transfer protocol with unified internetwork services associated with OSI Layers 3 and 4. XTP conforms to the architecture of the Transfer Layer in RTTS developed in France for use in LANs (see Section 5 of Appendix J). [Ref. GAM 1987] XTP is designed to support 100 Mbps sustained transfer rates between application programs with growth to 1 Gbps. XTP is designed to provide services for distributed systems not available in ISO TP4 and US DoD TCP; the requirements include supporting remote procedure calls and rapid request/response operations, coordinating multiple processes, and providing transaction-based file access. XTP supports traditional stream services, bulk transport, real-time reliable datagram service, real-time internet gateways, flow/error/rate control, message delivery confirmation, selective retransmission, message boundary preservation, multiple addressing plans, out-of-band signalling, reliable multicast mechanism, maintenance packets, and multipath capability. [Ref. XTP 1988, XTP 1989]

XTP has been submitted to ANSI X3S3 for standardization of its services. Its standardization is also being progressed in the US Navy SAFENET Committee.

17.5.4 EUROCOM and US/EUROCOM

EUROCOM. EUROCOM is a technical working group composed of representatives from the NATO European nations whose aim is to achieve better coordination and interoperability in tactical communications systems between European Allied armies. EUROCOM is a subgroup of the EUROGROUP, an informal grouping of European governments within the framework of NATO. Rather than trying to agree on a single system, it is EUROCOM's plan to introduce communications systems in accordance with agreed operational requirements and basic system parameters in such a way that there is complete interoperability among systems built to EUROCOM standards. EUROCOM standards are frequently offered as the basis for NATO STANAGs on tactical communications. [Ref. Manno 1989]

The documents (D) currently promulgated by EUROCOM include:

- EUROCOM D/0: *System Concept*, CONFIDENTIAL (date of last revision unknown)
- EUROCOM D/1: *Tactical Communications Systems Basic Parameters*, 1986 (Revised September 1988), RESTRICTED
- EUROCOM D/2: (title and date unknown) subject is testing.

EUROCOM systems are basically circuit-switched time division multiplexing (TDM) systems, with a basic channel rate of 16 kbps and delta [continuously variable slope delta (CVSD)] modulated voice transmission. Combinations of these channels are used to offer 32-kbps circuits and 256-kbps and 512-kbps trunks. Circuit-switched connections usually operate at 0.05, 2.4, or 9.6 kbps. An option is available for a packet switched data service. A set of Enhanced EUROCOM Standards (EESs) is being established, with a planned completion in 1994. These standards will address packet radio, message handling, and video. Among proposals being considered is variable-bit-rate transmission using a flexible forward error correction (FEC) scheme, enabling ATM to be used over noisy media such as radio transmission. [Ref. Valuer 1993]

US/EUROCOM. US/EUROCOM is an informal tactical communications technical working group comprising the EUROCOM nations and the United States, Canada, and France. The purpose of US/EUROCOM is to work toward better and less cumbersome interface arrangements, to monitor the implementation agreements on communications characteristics, and to promote cooperation in the procurement of equipment conforming to these characteristics. Much of the preliminary technical work leading to ratified standardization agreements is accomplished by this group.

With respect to work in OSI, the principal interest in US/EUROCOM is with the lower three layers. Currently, US/EUROCOM is in the process of modifying STANAG 4249, *The NATO Multi-Channel Tactical Digital Gateway—Data Transmission Standards (Packet Switching Service)*, to reflect the 1988 version of ITU-TS Recommendation X.75. US/EUROCOM is also investigating the application of the PICS-type proformas to the NATO multi-channel tactical digital gateway STANAGs. [Ref. Manno 1989]

On many occasions US/EUROCOM has accepted invitations from TSGCE to work on the NATO STANAGs for tactical communications (not just gateways) and interoperability issues. US/EUROCOM has made major contributions to STANAGs 4206-4211 and 4350. Both EUROCOM and US military standards are being considered for drafts of STANAG 4290, *Fiber Optics*. In each case the technical recommendations from US/EUROCOM are provided to TSGCE SG11 WG1 for further work, coordination, and distribution as draft STANAGs.

The work of US/EUROCOM in developing a profile for a tactical gateway for packet switching (STANAG 4249) was briefed to the TSGCE SG9/WG1 in the October 1989 meetings in Brussels. In addition, Norway provided a paper that suggested US/EUROCOM could undertake several tasks of interest to SG9. These include proposing PICS proformas for the STANAG 4206-4214 series (and possibly others, such as STANAGs 4290 and 5040); proposing tactical parts of the STANAG 4250 series; identifying profiles required by the tactical communities in NATO; and proposing NATO functional profiles for tactical applications. However, US/EUROCOM's role in developing profiles for NATO is still under consideration and has not been fully accepted by US/EUROCOM. [Ref. TSGCE 1991i]

17.5.5 Other Efforts

STANAG 4214, *International Routing and Directory for Tactical Communications*, may be applicable to ATCCIS technical standards; this standard is the responsibility of TSGCE SG11. TSGCE SG9/WG1 is looking at naming and addressing requirements and the applicability of STANAG 4214. STANAG 4249, *The NATO Multichannel Tactical Digital Gateway—Data Transmission Standards (Packet Switching Service)*, also the responsibility of SG11, addresses packet switching using a form of ITU-TS X.25; as such, this STANAG may also be applicable to ATCCIS technical standards. The EUROGROUP on Cooperation of Tactical Communications Systems (EUROCOM) is reported to be preparing a revised draft for STANAG 4249 based on ITU-TS X.25 and the draft TSGCE SG9 Functional Profile Guidelines document; such a draft would be submitted to SG11 as a contribution and developed into a STANAG.

17.6 Assessment

a. TSGCE has identified and assessed eight military features that need to be incorporated in civil OSI standards, but little detail has yet been released (e.g., in drafts of STANAGs 4251-4266) to show how these features can actually be addressed in military versions of OSI standards. There does not seem to be much value in a set of layer STANAGs that primarily catalogue ISO and ITU-TS standards.

b. TSGCE SG9 has an ambitious 18-month plan for progressing the NATO OSI data communications standards, but there is a need to reassess and revalidate the military features—clearly the deficiencies of 1991 civil standards are different from those identified in 1983. For example, great progress on internetworking has been made in ISO.

c. TSGCE SG9 has been successful in many areas (such as security and OSI management) for introducing military work into the civil standards bodies and affecting the capabilities of the civil standards. One of the useful approaches being taken by SG9 is the focus on the applicability and adequacy of civil profiles for use in NATO by addressing specific military scenarios and groups of requirements. Profile-oriented work is essential to ensure interoperability of implementations by the Nations. It is clearly the focus of the reorganization of SG9 that will be evolved in 1992. Current efforts on profiles need to be supported and expanded. This work should be in close coordination with the regional implementor's workshops (e.g., EWOS and the North American OIW), since NATO cannot afford to implement on a wide scale major variations of the profiles negotiated in the civil communities.

(This page intentionally left blank)

18. NEAR-TERM ANALYSES, INITIATIVES, AND SYSTEMS FOR ACHIEVING INTEROPERABILITY IN NATO

Quick Reference	
Topic	Page
ACE ACCIS	396
ACCS	399
AHWG on ATCCIS	395
Architectural Issues	420
BICES	404
C3 Restructuring	386
CNSI	414
ISDN Issues	428
NATO OSE Ref. Model	416
NATO Software Stds	431
NIDTS	414
NMOS	406
OSI Issues	425
PG6-Tac Comms 2000+	388
Quadrilat Interop Prog	408
STAMINA	410
TCP/IP-OSI Coex/Conv	419
TSGCE SG11	387
TSGCE SG12	393
WG2 on Data Proc/Mgt	394

TSGCE is developing recommendations and standards in two areas, in addition to the work of TSGCE SG9 on Data Distribution (described in Chapter 17), that could have significant impact for information systems. These are SG11 on Communications and SG12 on Information Systems.

Existing and emerging ACCISs are designed to provide command and control information support for NATO and national systems. The ACE ACCIS will provide the higher-echelon support (i.e., at echelons above corps) for the military forces operating in the European region of NATO. ATCCIS will provide support for land combat tactical units, and the Air Command and Control System (ACCS) will support the air operations.

The NATO Maritime Operational Intelligence Support (NMOS) and the Battlefield Information Collection and Exploitation Systems (BICES) will provide intelligence support. Other ACE ACCIS -related projects include the Standard Automated Message Interface for NATO's ACCISs (STAMINA), JRMS, the Status Control Alerting and Reporting System II (SCARS II), and the Nuclear Planning System (NPS).[92]

This chapter begins by reviewing the structure of the TSGCE and the work of TSGCE SG11 and SG12 (Section 18.1). It further examines the standards specified by near-term NATO and multilateral interoperability demonstration and development efforts in addition to ATCCIS, namely the ACE ACCIS (Section 18.2), ACCS (Section 18.3), BICES (Section 18.4), NMOS (Section 18.5), the Quadrilateral Interoperability Programme (Section 18.6), and STAMINA (Section 18.7).[93] Military features required by NATO are addressed. In addition, this chapter addresses some of the issues associated with evolving from near-term systems to ATCCIS through the use of standards. Profiles of standards that are to be used in transition implementations for several NATO projects are also presented.[94]

The objective of this review is to ensure that the methodology used for the ATCCIS effort is comprehensive and that no classes of relevant standards have been overlooked. Some national initiatives to adopt and extend OSI standards for tactical employment are reviewed in Appendix C.

---

92 ACCS, ATCCIS, BICES, JRMS, NMOS, NPS, and SCARS II are the seven ACE CCIS-related projects identified in the *ACE Inventory of Key Tasks* [Ref. ACE 1988].

93 The information provided in Section 18.2 through 18.7 was reviewed and updated by SHAPE staff in January 1992 and is to be updated again through further discussions in January and February 1994.

94 Profiles differ from stacks in that a profile usually consists of several stacks of standards and further that profiles are usually recommended for a certain transition strategy or a specific implementation. In some cases, profiles specify options to be used.

18.1 Standardization work in the TSGCE

18.1.1 Impact of NATO C3 Restructuring on TSGCE

C3 Restructuring. In January 1994 the TSGCE plenary and an informal meeting of the NACISC addressed proposals for restructuring the organization and responsibilities of the TSGCE and the NACISC and supporting elements. Three proposals were considered—none were adopted but none were found unacceptable. These proposals, derived from the Anderson Report of December 1993, were the following [Ref. Rannestad 1994]:

- Combine TSGCE and NACISC and constitute a C3 Management Board to oversee the work
- Combine STC and ADSIA and constitute an integration center
- Combine the International Military Staff (IMS), comprising about 85 people, and the International Staff (IS), comprising about 11 people,[95] into a C3 Directorate/Defence Board.

Impact on TSGCE. Reorganization of the TSGCE is being considered whether or not TSGCE and the NACISC are merged. The number of groups within the TSGCE has already been reduced from 60 to 35; reorganization would further reduce the number of groups to 12-16. The proposal from the TSGCE Chairman (also the UK position) January 1994 [Ref. Goldon 1994] suggested the following 16 groups for TSGCE:[96]

- Communications Standing Group derived from SG4, to address communications systems cooperation
  - WG on tactical (mobile) communications, derived from PG6
  - WG on strategic (fixed) communications, derived from SG9's AHWG on ISDN
  - WG on satellite communications, derived from SG11's WG8
  - PG on tactical spectrum management system, derived from PG8
  - Steering committee on Communications System/Network Interoperability, derived from SC on CSNI
- Information Systems Standing Group derived from SG4, to address information systems cooperation
  - WG on electronic mail and messaging systems, derived from SG9's AHWG on MMHS
  - WG on data links, derived from SG9's WG4
  - WG on information systems security, derived from SG9's AHWG on Security
  - WG on data processing and management, derived from SG12
  - WG on data fusion, derived from SG12
  - WG on software engineering, derived from SG12 and acting as a shared group with the NACISC
  - Steering committee for BICES Project Management Group, derived from SC on BICES
- Navigation Systems Standing Group, derived from SG4, to address navigation systems cooperation
- Identification Systems Standing Group, derived from SG5, to address identification systems cooperation

---

95 Several key people from the IS have left or will be leaving in the first part of 1994: Seifert (already departed), A. Rannestad, and L. Klein. Not all will be replaced.

96 The United States has recommended that SG12 be disbanded and its work be accomplished in the NACISC, not the TSGCE. At present, SG12 is dormant and its WG2 met only once in 1993 (February).

18.1.2 Work of TSGCE SG11 on Communications

TSGCE SG11 on Communications (1) promotes collaboration amongst the nations on projects to develop and produce common equipment and systems in the area of communications and (2) prepares required technical STANAGs for communications systems and equipment. The goal is to promote and achieve interoperability between national and NATO-funded systems, both tactical and strategic.[97]

18.1.2.1 Organization of SG11

At the November 1991 plenary of SG11, SG11 reviewed and approved the terms of reference and special tasking instructions for its subgroups and subordinate bodies. The organization of SG11 is as follows [Ref. Pilla 1991]:

- WG1 on Tactical Area Communications, which identifies interface requirements and prepares draft new or modified tactical area communications STANAGs in the areas of terminal, multiplexing, switching, and multi-channel radio equipment as well as interface gateways and devices among tactical systems, strategic systems, and commercial systems.
- WG2 on Narrow-Band Speech, which investigates possible speech techniques in order to achieve high quality (under adverse acoustical conditions) of reproduced voice in as narrow a frequency band as possible.
- WG3 on Tactical Communications Equipment for Use in the Maritime Environment, which identifies interface requirements and prepares draft new or modified STANAGs for secure submarine, air, and surface communications capabilities.
- WG5 on Single Channel Radio Systems, which identifies interface requirements and prepares draft new or modified STANAGs in the areas of single channel and combat net radios.
- WG8 on Satellite Communications Systems, which identifies interface requirements and prepares draft new or modified STANAGs in the areas of satellite communications.
- PG6 on Tactical Communications Systems for the Land Combat Zone—Post 2000, which is developing technology assessments, an agreed tactical communications architecture, a transition strategy, and standards.
- PG8 on Tactical Spectrum Management System, which is defining a NATO tactical spectrum management architecture and identifies opportunities to harmonize current systems.

18.1.2.2 Activities of the Working Groups

SG11/WG2 is planning tests for low-rate speed coders and will report results in 1992. Planning for testing other voice coders and error correction devices will be conducted in 1992.

SG11/WG5 is developing a STANAG for High Frequency (HF)/Electronic Counter-Counter Measures (ECCM); the initial draft for circulation to the nations is planned March 1992. Work has begun on VHF ECCM; a draft STANAG is being considered for VHF interim interoperability using gateways for analog voice. Other areas of interest to WG5 are HAVE QUICK II radios and SATURN radios (STANAG 4372) and the requirements for NATO

---

97 The information presented on the work of SG11 is very general. This is because more detailed information, including the special tasking instructions, reports of meetings, and most of the formal correspondence regarding SG11 is being classified as NATO RESTRICTED by the NATO Secretariat. Only material available at the unclassified level and appropriate for wide dissemination has been used herein.

Improved Link Eleven (NILE). WG5 reviewed STANAGs 4203, 4204, and 4205 in 1991 and will review STANAG 4202 in 1992.

Canada, France, Germany, the United Kingdom, and the United States have signed an MOU for work in SG11/PG8 on the Tactical Spectrum Management Program. Spain is also considering joining this program. [Ref. Howe 1991]

18.1.2.3 Work of PG6 on Post-2000 Tactical Communications[98]

The objective of the work of SG11/PG6 is to seek, through a coordinated program, tactical communications systems designed to common standards, to include collaborative work on subsystems and standards development, where appropriate. The result of the common standards and collaborative work on subsystems is expected to be the achievement of progressively enhanced interoperability.

PG6 has been working in seven areas: architecture, switching, communications media, mobile systems, terminals, system management, and security. This work was divided into three phases—planning, study, and integration—and has resulted in a description of the recommended post-2000 architecture, supported and justified by a number of detailed technology studies. Areas for standardization have been identified. The final product is the *Phase I Final Report* [Ref. TSGCE 1991j], which includes:

- An operational and architectural framework for tactical communications systems for the land combat zone in the post-2000 time frame
- A list of standards and areas for standardization work within this framework
- Proposals for the next stage of work.

The framework takes into account national and NATO military operational requirements and the SHAPE concept[99] for tactical communications in support of land operations. It is based on several pre-feasibility studies done by the NIAG (completed in 1990) and under a multinational MOU.[100] It describes the preferred architecture and identifies essential system (interoperability) parameters.

The report identifies standards and areas for standardization required for equipment development according to the preferred architecture. PG6 identifies the existing STANAGs that fit the architecture, the existing STANAGs that may need modification, and areas for standardization in which new STANAGs or other standards will need to be written.

The next phase of work encompasses defining the architecture in greater detail, to include the functional and performance aspects, in order to reach the level of detail needed to prepare the STANAGs, as well as the system- and subsystem-level specifications. In addition, PG6 is planning on a limited number of studies to enhance the base knowledge in rapidly changing or new technologies applicable to communications. The products for 1992-93 are expected to include (1) elaboration of the agreed architecture in more detail and (2) confirmation of the transition strategy.

---

98 Material in this section is based on a private communication with Sal Manno (US Representative to PG6), JTC3A, 9 December 1991.

99 Only drafts of the concept were completed during the first phase of the PG6 architectural work. These drafts have now been withdrawn and a new tactical communications concept is in preparation. When completed, ATCA intends to work on a military operational requirement based on the tactical communications concept.

100 The 1991 participants in the MOU were Canada, France, Germany, Italy, the Netherlands, Norway, Spain, the United Kingdom, and the United States. The MOU covers a number of pre-feasibility studies that extend the work completed by the NIAG. Portugal as indicated interest in joining the MOU for work in 1992.

For the period 1994-1997, the emphasis in PG6 will be on the development of standards for the post-2000 era.

SG11 has agreed that PG6 be given the systems engineering responsibility for all SG11 work related to the PG6 tactical communications system architecture and that SG11 manage all the SG11 work and schedules within the framework of that architecture. The overall concept was endorsed by SG11 in November 1991, and PG6 was requested to provide a comprehensive work plan for submission to SG11. [Ref. Manno 1991a]

SG11 has been asked by the TSGCE to provide a schedule at the January 1992 TSGCE plenary for the completion of two CNAD tasks: (1) interoperable communication links for tactical headquarters and (2) interconnection of tactical and strategic communications systems. SG11 has also been asked by the TSGCE to assist in expediting agreements necessary to make HAVE QUICK IIA algorithms available to SATURN radios and to respond to a Conventional Armaments Plan tasking for a second generation ECCM UHF program (and report to the TSGCE in June 1992). [Ref. Howe 1991]

18.1.3 Communications Architecture Post-2000

PG6 was initiated in 1989 under a memorandum of understanding entitled, "Cooperative Pre-feasibility Studies for Tactical Communications Systems for the Land Combat Zone—Post 2000." The aim of PG6 is the development of standards recommendations—based on current and future civil standards—for a land-based, interoperable tactical communications system for the post-2000 era. The first phase of PG6 was completed at the end of 1991 with the recommendation of an architecture, designed to be extremely flexible and making use of advanced telecommunication developments in the military as well as civilian environments. The second phase, now underway, is focused on refining the architecture and adding standardization areas; it is expected to be completed in the first half of 1994. [Ref. Thieme 1993]

The architecture addresses such requirements as [Ref. Valuer 1993]:

- Increased mobility of military forces, requiring a communication system with an extremely high degree of mobility and economy
- Higher degree of assured availability and security for mobile users
- Introduction of advanced C3I, requiring high bit-rate systems, at least within headquarters, and hence more flexible use of the available bandwidth, to include both high-speed data and video communications
- More extensive use of computer systems and data, requiring interfaces to mobile users (e.g., via packet radio)
- Automated message handling system with connections to the public X.400 service
- Radio relays with higher bandwidth and lower probability of enemy detection, obtained from use of higher frequency (e.g., 60 GHz) transmissions
- Operability between military units from different nations, requiring fully interoperable communications systems with attendant network management services.

The architecture includes a multi-role radio that can be used for single-channel radio access (SCRA), combat net radio, and packet radio applications, in both voice and data transmission modes. The architecture recommends the asynchronous transfer mode (ATM) for basic switching and transmission, enabling efficient and dynamically responsive use of available bandwidth. Telecommunications management network (TMN, CCITT M.30), based on an object-oriented approach, and CMIS/CMIP are recommended for network management services. The Local Area

System (LAS) component of the architecture covers communication needs of a tactical (corps, division, and brigade) headquarters, for which staffs are expected to be distributed (e.g., over an area of one square kilometer). Staff sections would be equipped with a small ATM node with broadband interconnections over fiber optic cables or 60-GHz radio relays, giving trunk capacities in the order of 100 Mbps. LAS subscriber connections would use either the EUROCOM "K" interface, ISDN basic access, or broadband ATM interface at about 20 Mbps. The need for TCP/IP stacks as well as OSI stacks is recognized as part of the transition strategy. The Wide Area Subsystem (WAS) is designed to cover an entire theater of operations with a truck network, using such technologies as variable-bit-rate transmission, dynamic anti-jamming, and other electronic counter-countermeasures. Long-distance, line-of-sight radio relays in the UHF to SHF bands will be capable of bit rates of 2-10 Mbps. Troposcatter and satellite communications may also be used as a supplementary overlay for direct interconnection of nodes extremely far apart. WAS will not offer broadband ATM; hence, data and video communications will be limited to about 64 kbps, which can be handled by ISDN. Mobile User Subsystem (MUS) subscribers will use a Multi-Role Radio (MRR) and interconnect with the WAS using radio access points (RAPs) connected directly to a switch port in a LAS or WAS.

PG6 has conducted analyses, modelling, and simulation to explore the feasibility of the standards recommended in the architecture. One of these (conducted by TNO [Ref. Thieme 1993]) explored the use of DIS 8802-6 (IEEE 802.6)—a MAN standard also known as distributed queue dual bus (DQDB)—for the LAS command post network. Requirements for the LAS include:

- Survivability that guarantees operation of the LAS by minimizing effects of faults be means of:
  - Automatic by-passing or isolation of faulty stations
  - Built-in redundancy and alternative paths (back-up links)
  - Automatic reconfiguration and rerouting
  - Stand-alone operation of any non-damaged part of the network
  - Low probability of intercept (LPI) and detection
- High mobility so as not to restrict tactical operations
  - Automatic by-passing or isolation of faulty stations
- Levels of precedence to allow timely information exchange under all combat conditions, including seizure (preemption) of transmission service, assets, and terminals used to serve lower-precedence levels
- Multimedia transmission support, including speech, data communications (text, graphics, speech, high-definition pictures, and video), and video communications (video telephony and video conference).

The TNO study, modelling, and simulation had positive conclusions on the use of the DQDB MAN standard. DQDB based on fiber optic transmission systems can be a good basis for LANs in the LAS. Within a DQDB bus, millimeter-wave transmission systems can also be used, but it is not very effective to use more than a few radio links on a bus that used the DQDB protocol. When building a more complex network to support dispersed command posts, several DQDB subnetworks should be used that can be coupled using millimeter-wave radio transmission means. The available speeds of DQDB (155 Mbps) are sufficient to achieve the desired quality of service. Finally, additional research is needed to enhance the standard so that it will be able to (1) keep isochronous connections during reconfiguration of the bus and (2) use a common priority mechanism for connectionless and isochronous service.

18.1.3.1 NATO Tactical Communications Architecture Post-2000

The major components of the NATO Tactical Communications Architecture Post-2000 being developed by PG6 are a Local Access Subsystem (LAS), a Wide Area Subsystem (WAS), and a Mobile Subsystem (MS). Figure 22 depicts an extended LAS component with three interconnected LASs.

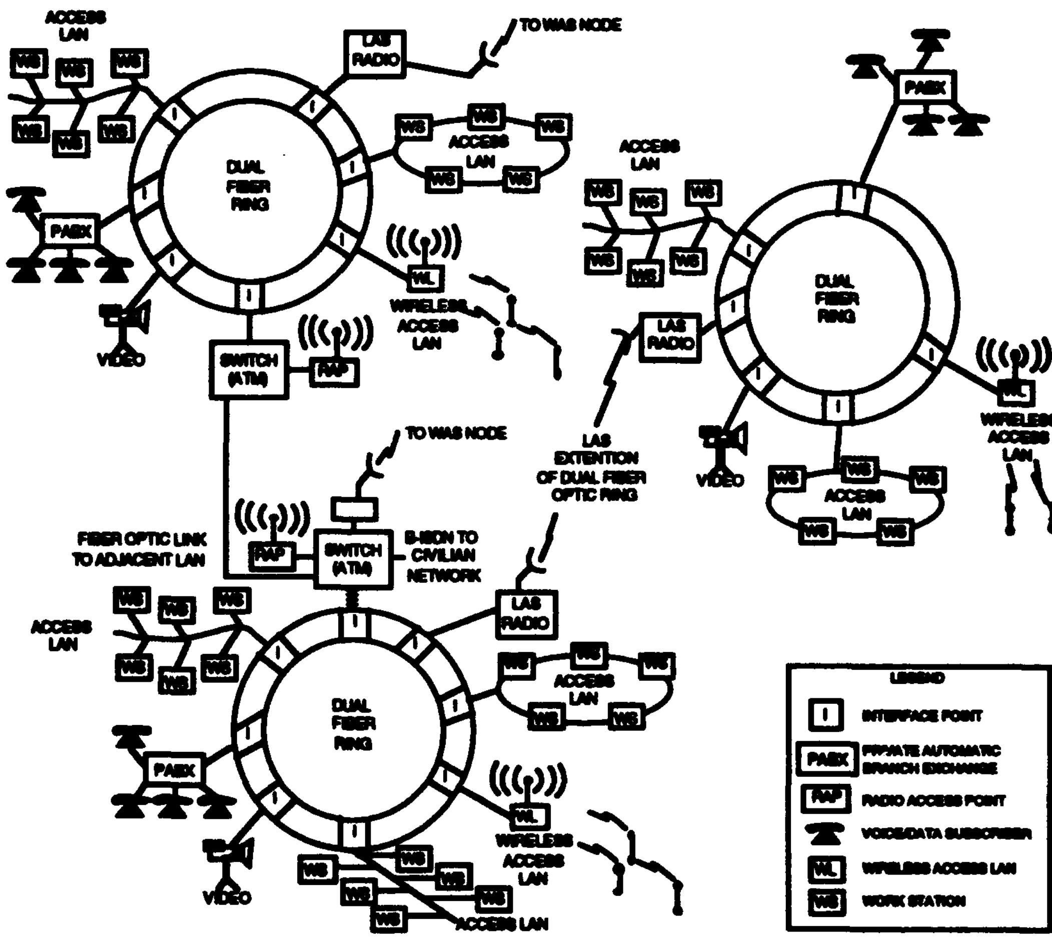


Figure 22. Post-2000 Tactical Communications Architecture-Extended LAS

The LAS provides the means for user access to the WAS and for local communications services in the local area. Additionally, it provides interfaces to the civilian commercial network. The LAS is composed of distributed access LANs and centralized access PABXs connected by dual fiber optic rings (see Figure 22). The access LANs provide service access for a distributed community of interest to the dual ring LAN, while the PABXs represent the interconnection of existing switching equipment to the new network. The PABX will be phased out and replaced by LAN technology as the architecture evolves into the future. The dual ring LAN has a wide-band Asynchronous Transfer Mode (ATM) switch that provides access to other LAS rings via a LAS radio or to the WAS nodes via WAS radio links. The LAS radio is also used, as well as fiber optic cable, to extend the dual ring in the event of a geographical obstacle. User access to the LAS is via a single channel providing integrated (voice, data, and video) services either separately or

simultaneously. User terminals are envisioned to function similarly to commercial ISDN terminals, using ISDN-type signalling and message sets modified for tactical use to control and request access to integrated user services.

The WAS provides long-haul transport and switching of user services through the tactical network as well as local access to users in the vicinity of a WAS node. WAS nodes are really extensions (explosions) of the LAS architecture with longer-range transmission and greater variety and number of transmission resources. ATM technology is used to replace fixed-bit-rate circuits with flexible virtual circuits in which capacity is negotiated on an as-needed basis. The ATM capability of the WAS architecture will replace current-generation circuit, packet, and message switches with fast "asynchronous" packet switches. These switches will be linked by wideband trunks in which the full capacity of the radio link will be available to the switch as a single wideband circuit rather than multiplexed narrow-band time-division-multiplexed circuits. The ATM switch will statistically multiplex the instantaneous demand for virtual circuit service from diverse end users on this single wideband channel.

18.1.3.2 Post-2000 NATO Reference Model

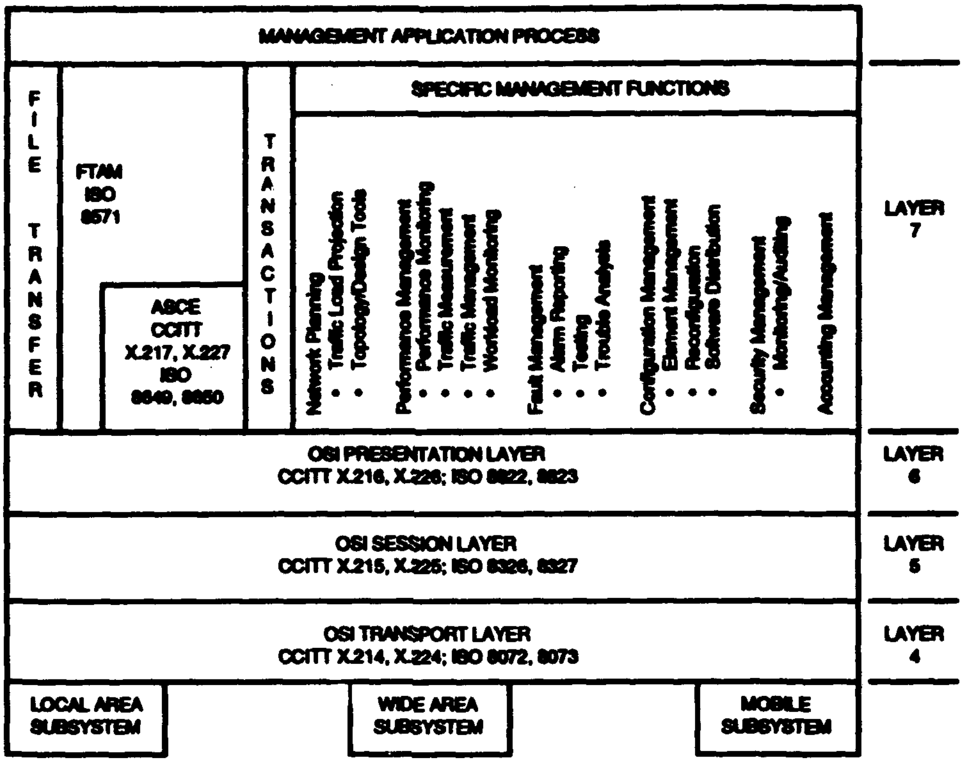
PG6 has also developed a conceptual Post-2000 NATO Reference Model for use with the future tactical communications architecture with seven layers (not identical with the OSI and current NATO Reference Model): Media Layer 1, Access Layer 2, Routing Layer 3, End-to-End Layer 4, Session Layer 5, Presentation Layer 6, and Application Layer 7. The upper layers and the protocol stacks envisioned for network management protocols for the Post-2000 Tactical Communications Architecture are shown in Table 59.

18.1.3.3 NATO C3 Physical Communications Architecture

In May 1992, NACISA published the *NATO C3 Physical Communications Architecture–Recommended Topology* [Ref. NACISA 1992], which established a generic switched network architecture for the 1990s. For NATO's circuit-switched needs, the study recommended that NATO should field a hybrid network consisting of three components: (1) a NATO Core Network (NCN) consisting of integrated services PABXs (ISPABXs), (2) services provided by national defense networks, and (3) public switched telephone network (PSTN) services. The primary purpose of the latter two components was to provide cost-effective service for remote NATO subscribers, alternate routing, overflow capacity, and increased survivability. The size of the NCN and the degree of services sought from the national defense and PTT networks was to be based on the most cost-effective solution. [Nevergold 1993]

A number of conclusions can be drawn from the studies and analyses of [Nevergold 1993]. Given the technology existing today, NATO's circuit-switched communications needs are best served by a hybrid network consisting of a NATO Core Network that (1) provides switched services to users located at major NATO headquarters, (2) interconnects national defense networks, and (3) uses national PTT networks to increase survivability and accessibility to remote users in a cost-effective combination. The cost of the NATO Core Network is driven by transmission costs. Total network cost is largely independent of the number of core switches in the range of interest; therefore, other considerations such as survivability, availability and subscriber access, which can vary with the number of switches, can be improved without adversely affecting cost.

Table 59. Proposed NATO Post-2000 Network Management Protocols



Source: *Subjective Evaluation of Candidate Architectures for the Tactical Communications Systems Land Combat Zone Post 200*, Draft, Prepared by the United States for TSGCE PG6, 10 May 1991, NATO UNCLASSIFIED.

18.1.4 Work of TSGCE SG12 on Information Systems[101]

TSGCE SG12 on Information Systems was established[102] by the TSGCE to (1) promote and enable collaboration among the nations of the Alliance on projects to develop and produce common equipment and systems in the area of information systems and (2) provide technical standards in the area of information systems. The goal was to promote and enable the achievement of interoperability between and among national and NATO-funded CCISs, both tactical and strategic. SG12 has two subordinate bodies, which will establish a close working relationship with each other:

- WG2 on Data Processing and Management, which will recommend standards on data processing and security with ADP systems.
- AHWG on an Army Tactical Command and Control Information System (ATCCIS), which is emphasizing data management and exploiting the Phase I and Phase II technical work on a standards-based architecture during 1984-91 by France, Germany, the United Kingdom, and the United States.

101 This section is based on the *Report to the Tri-Service Group by the Chairman of the Subgroup on Information Systems*, AC/302(SG/12)D/7, 21 November 1991, NATO UNCLASSIFIED.

102 Neither SG12 nor its only working group (WG2) met in 1993 due, in part, to concern by some nations (notably the United States) that work of SG12 overlaps the responsibilities of the Information System Working Group of the NACISC. This overlap is the subject of further discussions for restructuring NATO standardization bodies.

Two other TSGCE groups, originally assigned to SG12 during the initial work on TSGCE restructuring, have now been directed by the TSGCE to continue reporting directly to the TSGCE. They are the Project Group (PG7) on BICES and the Special Working Group on Ada Programming Support Environment (APSE) (this group had been renamed Working Group on Software Engineering when it was considered part of SG12). Eleven nations have been participating in the MOU on BICES and two others are expected to join. The Working Group on Geographic Information Systems, initially assigned to SG12, has been transferred to the Military Agency for Standardization (MAS).

18.1.4.1 WG2 on Data Processing and Management

Table 60 shows the special tasking instructions for WG2 that govern its work. The initial program of work for SG12/WG2 is as follows [Ref. TSGCE 1991m]:

- Data Management Reference Model (DMRM) and Architecture
  - Monitor the status of work in ISO and other relevant international standardization groups
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging NATO Data Management Policy.
  - Determine, by reference to recognized user representatives at the strategic and tactical levels, the requirements for the NATO DMRM and architecture.
  - Identify the possible options for the selection of a NATO DMRM and architecture and make appropriate recommendations.
  - Time scale and milestones are to be determined; lead nation is France.
- Data Models
  - Monitor the status of work in OSI and other relevant international standardization groups.
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging NATO Data Management policy.
  - Determine, by reference to recognized user representatives at the strategic and tactical levels, the requirements for data models and in particular make recommendations as to the number and type of distinct models required.
  - Determine the requirements for the production (by others) of an initial data model(s) and for subsequent maintenance of that model(s).
  - Identify a suitable set of software tools and aid packages to assist in the creation and maintenance of such models, and make appropriate recommendations.
  - Time scale and milestones are to be determined; lead nation is the United Kingdom.
- Data Dictionaries
  - Monitor the status of work in ISO and other relevant international standardization groups.
  - Determine, by reference to recognized user representatives at the strategic and tactical levels, the requirements for data dictionaries.
  - Determine the requirements for the reproduction (by others) of an initial data dictionary from the NATO Data Model(s) and for subsequent maintenance of that dictionary.
  - Identify the possible options for the selection of a NATO standard for data dictionary definition, and make appropriate recommendations.
  - Define the structure of a NATO data dictionary using an appropriate meta-language.

- Identify a suitable set of software tools and aid packages to assist in, or to automate, the process of converting a data model into a set of data definitions for incorporation into a NATO data dictionary.
- Be prepared to respond to specific queries by the provision of technical advice to staff responsible for the management of the NATO data dictionary.
- Time scale and milestones are to be determined; lead nation is the United Kingdom.

• Data Definition and Data Schemata
  - Monitor the status of work in ISO and other relevant international standardization groups.
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging Data Management Policy.
  - Determine by reference to recognized user representatives at the strategic and tactical levels, the requirements for data schemata.
  - In consultation with appropriate NATO and National Staff, determine the requirements for the production and subsequent maintenance of data schemata.
  - Identify a suitable set of software tools and aid packages to assist in, or to automate, the process of generating data schemata from a NATO data dictionary, and make appropriate recommendations.
  - Be prepared to respond to specific queries by the provision of technical advice to staff responsible for NATO projects.
  - Time scale, milestones, and lead nation are to be determined.

• Data Access and Manipulation Standards
  - Monitor the status of work in ISO and other relevant international standardization groups.
  - Review the products of other relevant study groups, with particular reference to the ATCCIS study and the emerging NATO Data Management Policy.
  - Identify the possible options for the selection of NATO standard access and manipulation languages, and make appropriate recommendations.
  - Identify software tools and aid packages appropriate to assist, or to automate, the generation of applications from initial analysis and outline definition of functional requirements (CASE tools), in conformity with the standards recommended. (This activity is seen as providing guidance and is not to be taken to imply that the Working Group will endorse any particular products nor undertake any form of market survey.)
  - Time scale, milestones, and lead nation are to be determined.

18.1.4.2 AHWG on ATCCIS

The SG12 AHWG on ATCCIS held its first meeting on June 1991 (this group is now inactive, having not met in 1992 or 1993). The meeting was organizational and focused on the relation of the existing ATCCIS groups (specifically the Permanent Working Group and its two subordinate groups, the Operational Subgroup and the Technical Subgroup). It was noted that the Operational Subgroup is currently meeting (with additional national participation from Canada and the Netherlands) as an ad hoc working group under the Operational Procedures Working Party of the MAS Army Board. One suggestion was that the AHWG on ATCCIS similarly meet with all interested national participation simultaneously with the existing ATCCIS Technical Subgroup, which would avoid creating a new standards body and resulting overlapping efforts. In September 1991, the TSGCE noted a recommendation that SHAPE retain operational sponsorship of ATCCIS, that the existing ATCCIS groups remain in effect, and that a relationship between ATCCIS and the TSGCE be established. The terms of reference for the AHWG on ATCCIS, as

well as the terms of reference for SG9, SG11, SG12, and their subordinate bodies, were reviewed by the TSGCE in January 1992. [Ref. Howe 1991]

Table 60. Proposed Tasking Instructions for SG12/WG2 on Data Processing and Management

1. The working group shall adopt the following definition of Information Systems for the purpose of defining the scope of its activities: Data processing systems which are used in support of C3I processes within NATO and the nations, excluding embedded systems within sensor systems and weapons platforms. The requirements of development systems (for developing hardware and software) shall be excluded from the scope of the Working Group.
2. The Working Group shall work in close association and harmonization with the SG12 Working Group on Software Engineering.
3. The Working Group shall ensure that all STANAGs developed by the Group are based to the greatest extent possible on existing or emerging civilian standards.
4. The Working Group is required to undertake the following tasks:
   a. Maintain a corporate up-to-date knowledge of present and planned NATO and national data processing and management systems.
   b. Identify, review, and prioritize the requirement for standards for data processing and management systems.
   c. Take account of related activities in NATO and in particular the activities of TSGCE SG9 and its subsidiary bodies; AC/317, including ISWG, ADSIA, ACCSA, and NACISA; AC/35; STC; DRG; Inter-Service Geographic Working Group; and establish effective means of liaising with these and other bodies, both within and outside NATO (such as ISO), so as to establish prioritized requirements and avoid duplication of effort and activities.
   d. Identify and review existing and emerging standards for data processing and management systems to enable it to make recommendations for the adoption or enhancement of these standards for collaborative NATO and national projects, consistent with meeting the identified minimum military requirement and in accordance with authoritative advice and policy on security matters from AC/35 and ACCSA.
   e. Develop STANAGs, in accordance with these recommendations, to ensure interoperability of NATO and national data processing and management systems.
   f. Promote measures for improving the efficiency of, and reducing the cost of, the procurement, operation, and maintenance of NATO and national data processing and management systems including, where appropriate, the development of STANAGs.
5. The Working Group shall report at regular intervals to SG12 and produce a forward plan of work for agreement by the Subgroup. This work plan is to identify both the areas of interest of the Working Group and the documents which will be produced as deliverable outputs to the Subgroup.

Source: *Tasking Instructions for the Working Group on Data Processing and Management*, Appendix 2 to Annex III to AC/302-D/616, *Report to the Tri-Service Group by the Chairman of Subgroup on Information Systems*, AC/302(SG/12)D7, November 1991, NATO UNCLASSIFIED.

The proposed tasks of the AHWG on ATCCIS were to [Ref. ATCCIS 1991]:

- Assist the TSGCE in identifying standards or standards parameters required for interoperability of tactical land force ACCIS as identified in the ATCCIS effort.
- Review and coordinate ATCCIS working papers for TSGCE acceptance and promulgation.
- Document and address key technical standards issues attendant to the emergence of ATCCIS conformant systems.

18.2 ACE ACCIS

The term "Allied Command Europe—Automated Command and Control Information System" (ACE ACCIS) reflects the intended aim of a common ACCIS architecture to be applied in a uniform way across ACE (i.e., to provide automation support for NATO Headquarters at echelons above corps).

Current ACE ACCIS Specifications. The following are the key documents in defining the future work by NATO on ACE ACCIS:

- *ACE ACCIS Implementation Strategy (AAIS),* NACISC, June 1993 [Ref. ACE ACCIS 1993a]
- *ACE ACCIS Target Architecture,* Director General NACISA, September 1993, NACISC, June 1993 [Ref. ACE ACCIS 1993b; ACE ACCIS 1993c]
- *ACE ACCIS Core Capability and Capability Increments,* Draft for SHAPE Coordination, NACISC, January 1994 [Ref. ACE ACCIS 1994a]
- *NATO Open Systems Environment (OSE)—Baseline Architectural Principles and Reference Model,* NACISC/ISWG, July 1993 [Ref. NATO OSE 1993]
- *NATO Data Management Policy,* AC/317-D/61, NACISC, June 1993, [Ref. NACISC 1993a] (approved by the CSWG/ISWG with the following caveat: that the formal attribution of the specific tasks to the TSGCE, within the policy document, is not currently agreed and that the formal attribution of these tasks will be finalized once the wider issue is resolved as a result of the accepted outcome of the C3 Restructuring Study).

Architectural Design Study. A major ACE command and control information system study—the *ACE Architectural Design Study (ADS)*—was conducted between March 1980 and 1982. The aims of the ADS were to:

- Identify those command and control related activities of the ACE headquarters that lend themselves to ADP support
- Consider the additional requirements of interfaces to national systems, communications, and resources
- Define an ADP architecture that provided the required support to command and control in the "most operational and cost effective way"
- Define an implementation strategy to provide early implementation at an acceptable cost and effort.

System Design and Integration Contract. The system definition project for the ADS was known as the System Design and Integration Contract (SD&IC). The contract was let to a multi-national consortium and was originally planned to cover the period from 1989 throughlate 1991. Although the study was ACE-wide, it concentrated on SHAPE and the Central and Southern Regions, taking account of the need for interoperability, economy, and manpower. The SD&IC attempted to develop, as far as possible, a common system design for ACE ACCIS.

The SD&IC had two major objectives: (1) to complete the system architecture for ACE ACCIS and (2) to prepare for the next generation of ACE ACCIS nodes in SHAPE and the Central and Southern Regions.

Due to unforeseen difficulties the SD&IC fell behind in time scale and budget, which when combined with a changing political and military situation, resulted in some of the products no longer meeting the "current" situation.

The difficulties experienced in concluding the SD&IC resulted in the contract being terminated before completion and the emphasis being placed on evolutionary acquisition of ACE ACCIS as defined in the AAIS, which defines the implementation of individual ADP systems building toward an agreed architecture.

STC Testbed Laboratory. STC has developed a testbed laboratory[103] designed to demonstrate concepts for ACE ACCIS and other headquarters information systems (HISs). Initially the testbed provides a message handling network interconnecting headquarters units that have very different message and decision support functionality. Some units are assumed to be limited to generation and display of message text formats, while others are capable of storing messages in command databases and exchanging decision support data (such as graphics displays). The testbed is based on commercial off-the-shelf products (e.g., SUN, UNIX, and X-Windows) and is capable of [Ref. STC 1991a]:

- Message handling over NATO TARE and OSI networks
- Support of generic user functions such as briefing contributions and message processing
- Interoperability with other CCISs, including transfer of decision support data.

The network for these capabilities is the NATO TARE wide area network supported by a SHAPE Information Flow (SHIF) gateway to workstations, personal computers, and other command and control systems [e.g., Limited Operational Capability—Europe (LOCE)].

STC is using for its laboratory two prototype CCIS configurations. The War Headquarters Information Dissemination and Display System (WHIDDS) is installed in the SHAPE bunker command room to interconnect the staff cells with a central Headquarters database (based on DEC-VMS, DECNet, and FORTRAN 77). Another system, LENA-2, was developed at STC and is being maintained by SHAPE. An integrated CCIS, LENA-2 is designed to support the Alternate War Headquarters (AWHQ) or other HQ CCIS requirements. LENA-2 is based on SUN, UNIX, and X-Windows. Interoperability for the testbed laboratory is via X.400 and ADatP-3 messages.

ACE ACCIS Target Architecture. The ACE ACCIS Target Architecture consists of an architecture baseline, ACE-level architecture, node-level architecture, security architecture, discussion of system management, and recommendations on implementation-related standards. The baseline identifies the following elements and supporting mechanisms as essential:

- Interoperability between ACE ACCIS nodes—message exchange, E-mail, exchange of data files, and exchange and access of database data
- Interoperability with external systems—message exchange and, where possible, exchange of data files with information systems supporting rapid reaction and tactical forces, with other NATO and national systems, and with civil and public systems
- Common applications—message handling, message processing, E-mail, briefing support, significant event handling, tasker handling, document handling, data views, map graphics, time management, and office automation
- Special applications—mechanisms are to be defined.

ACE ACCIS systems are expected to be designed and implemented from a common architecture, including a common set of standards to ensure technical interoperability and portability of application software--both the architecture and standards follow the recommendations and principles of the NATO Open System Environment (OSE) [Ref. NATO OSE 1993]. Node system databases are to be based on common data definitions to ensure operational interoperability; common data will be defined in an ACE data dictionary and maintained by an ACE data administration capability. ACE ACCIS will follow the policy provided by the *NATO Data*

---

103 The testbed laboratory is, in part, an outgrowth of an ATCCIS Testbed developed by STC in support of the ATCCIS Phase II program.

Management Policy [Ref. NACISC 1993a], *NATO Interoperability Management Plan* [Ref. NIMP 1988], *NATO Interoperability Planning Document* [Ref. NIPD 1993], and *ACE Security Directive* AD 70-1.

The ACE ACCIS adopts the NATO OSE Reference Model, which is identical to the POSIX OSE Reference Model (P1003.00 [Ref. IEEE 1992] and which is shown (with some additions as a third "depth" dimension) in Figure 1 provided in Chapter 1. The NATO OSE standards applicable to ACE ACCIS are identified in Table 61.[104]

Table 61. NATO OSE Standards Applicable for ACE ACCIS

SERVICE AREA	NATO OSE STANDARD		
	Recommended	Emerging	Temporary
Programming			
• Programming languages	Ada, C		
• CASE		ECMA PCTE, EIA CDIF	
• Methods		SA, SD, HOOD	
User Interface			
• Graphical user interface			X-Windows
• Look & feel/toolkit			OSF/Motif
Data Management			
• Dictionary			ANSI IRDS
• DBMS	SQL	SQL2	
• Distributed data		RDA	
Data Interchange			
• Documents	ODA/ODIF/ODL, SGML/SDIF		
• Graphics	CGM	Raster Graphic Component	
• Electronic data (messages)			FORMETS (ADatP-3)
Graphics			
• Two-dimensional	GKS		
• Three-dimensional	PHIGS		
Network Services			
• Profiles	NOSIP		
• Message handling	X.400		
• Directory	X.500		
• Military message handling		STANAG 4406	
• OSI Layers 2-7			Internet Protocol Suite
• Network management		CMIS, CMIP, X.700	SNMP
• File Access	FTAM		
Operating System			
• Kernel OS API	POSIX.1		
• Commands/utilities	POSIX.2		
System Management		CMIS, CMIP, X.700	

Source: *ACE ACCIS Target Architecture* [ACE ACCIS 1993c].

18.3 Air Command and Control System (ACCS)[105]

The Air Command and Control System (ACCS) is a system to support air operations planning, tasking, and execution throughout ACE from Major NATO Command (MNC) level to

104 Annex B of the *ACE ACCIS Target Architecture* [Ref. ACE ACCIS 1993c] provides detail and rationale regarding the NATO OSE [Ref. NATO OSE 1993] standards applicable to ACE ACCIS.

105 Revised January 1994 based on [Rudderham 1994], [Stewart 1994], and [NACMA 1993b].

combat unit level.[106] ACCS will interface with the ACE ACCIS at the Principal Subordinate Command (PSC) and Allied Tactical Air Force (ATAF) and will concentrate on new development at the PSC and below. ACCS will progressively replace a current federation of individual systems that support ACCS functions to varying degrees.[107] At the PSC level and above, ACCS functions will be performed by the ACCIS of each Command.

Development of ACCS, which integrates offensive and defensive air command and control functions, has been underway for several years. Implementation is planned for the late 1990s. In April 1989, the ACCS Team delivered the partially completed the ACCS *Master Plan*. The ACCS Team was replaced by the ACCS Interim Management Group and later by the NATO Air Command and Control System Management Agency (NACMA). NACMA has conducted a system definition phase. System specifications and technical estimates were prepared in 1993 to support subsequent procurement of system entities.

Several levels of operational capability (LOC) are being defined for ACCS. LOC1, the first level of interoperability, is planned for the 1998 time frame. MIDS/Link 16 is an inherent feature of the ACCS design and may be incorporated in the LOC1 implementation. ACCS will use Link 16 for ground-air-ground tactical data exchange communications and Link 21 [formerly Link in Support of ACCS (LISA); also formerly Link 1 replacement] for ground-to-ground bit-oriented data exchange. NACMA is coordinating the introduction of MIDS/Link 16 into ACCS and has initiated a study on the operational, technical, and financial implications of the implementation of Link 16 in ACCS. [Ref. Maes 1991]

The interoperability concept for ACCS is discussed in Volume IV, *Generic Portion of the Overall* ACCS *Design,* of the ACCS *Master Plan* [Ref. ACCST 1986], and in the *Supporting Document on Organization Components* [Ref. ACCST 1988]. ACCS interoperability is planned through exchange of information through commonly agreed information definitions, formats, and technical standards. Where possible, the standards to be used are those developed by the Military Agency for Standardization (MAS), ADSIA, and TSGCE SG9. Specifically, ACCS will be based on the OSI Reference Model as specified in STANAG 4250 (NATO Interoperability Model), the OSI services for Layers 1 through 7 as specified in STANAGs 4251-4257, and the OSI protocols for Layers 1 through 7 as specified in STANAGs 4161-4267. In addition to the ISO Reference Model standards, the NATO Common Interface Standards will be used. TSGCE SG9 is responsible for the OSI technical standards, and ADSIA is responsible for the procedural standards. Operational interoperability standards will be based, in part, on Allied Tactical Publications (ATPs).

The ACCS communications concept is to integrate the various NATO and national dedicated communications systems currently used to support air operations into a common user data and voice network. ACCS would be hosted on the existing and planned communications without ACCS-unique communications means. Initially a packet switched data communication overlay would be added to the circuit-switched voice system. Continued support for both

---

106 The seven ACCS major functional areas are: Force Management (FM), C2 Resource Management (C2RM), Airspace Management (AM), Surveillance (S), Air Mission Control (AMC), Air Traffic Control (ATC), and Information Exchange.

107 The systems include Improved United Kingdom Air Defense Ground Environment (IUKADGE), Systeme de Traitement et de Representation des Informations de Defense Aerienne (STRIDA), German Air Defense Ground Environment (GEADGE), and NATO Air Defence Ground Environment (NADGE).

character-oriented and bit-oriented messages is required. Specifically, use of tactical data link standards such as Link 4, Link 6, Link 11, Interim JTIDS Message Standard (IJMS), and Link 16 would continue through the foreseeable future.

ACCS has been reviewing technical information exchange standards and requirements, including the need to replace Link 1 for data exchange[108] in the ground environment. The current approach is to base a new standard on STANAG 5516 (J-Series messages) and to develop (within the ADSIA Data Link Working Group) new or modified messages to fulfill specific ACCS Information Exchange Requirements. ACCS plans to use a military version of X.25 for packet-switched systems and for transfer over dedicated circuits and through circuit switches. Variable packet lengths are desired. CSMA/CD and token ring LANs are being considered for ADP systems. As in ATCCIS, the ACCS database concept is partitioned and partially replicated. An ACCS-wide data dictionary is planned. Analysis has included an STC investigation on the applicability of ASN.1 and its relation to the syntax of STANAG 5500/ADatP-3 (FORMETS). There is a concern as to whether use of FORMETS would permit achieving the full benefit of the OSI model.

The following considerations in ACCS indicate some elements of the technical approach for achieving interoperability:

- ACCS interfaces will be required to the following generic external agencies/systems:
  - NATO intelligence systems (e.g., BICES, NMOS)
  - NATO army headquarters
  - NATO land-based maritime headquarters
  - NATO maritime forces afloat
  - National headquarters, intelligence, army headquarters, maritime headquarters, territorial commands, meteorological services, civilian air traffic control, and local authorities.
- Requirements have been identified for free text traffic (electronic mail), graphics, and facsimile transmission services. Video transmission is a potential long-term requirement for ACCS, but it has been excluded from consideration for the current ACCS planning time frame (1990s).
- Two ADSIA standardization documents have been considered important for ACCS in the area of formatted messages:
  - ADatP-3/STANAG 5500, containing a catalogue of character-oriented formatted messages
  - Common Information Exchange Glossary (CIEG), containing terms and definitions applicable to the development of both bit- and character-oriented procedural standards.
- ACCS requires an electronic mail service. The planned standard is the Military Message Handling System, based on ITU-TS X.400.
- ACCS further requires automated interactions between databases (e.g., updates) that could be event driven. The FTAM standard has been recommended for consideration for ACCS use, particularly for bulk update of databases.
- The functions (e.g., syntax and formatting rules) of ASN.1 and the associated Basic Encoding Rules (BER) were recognized by the ACCS Team as potentially richer and offering greater scope than NATO Message Text Formatting System (FORMETS)

---

108 The ADSIA Data Link Working Group (DLWG) has been given a Priority One task to develop a Link 1 replacement; ADSIA DLWG has asked TSGCE(SG9) to look at media-independent protocols for such a concept.

functions of ADatP-3/STANAG 5500. Large investments in FORMETS are being made in operational systems, and NATO interoperability continues to be based on FORMETS and ADatP-3. Eventually, however, FORMETS could be replaced by ISO standards for automated data exchange to make better use of the functionality of the OSI model and the richness of ISO standards. There are potential problems in ensuring interoperability between systems using FORMETS and systems using ISO standards. Investigation is needed on whether the use of an information structure based on ADatP-3 message contents is a sufficient basis for achieving backwards interoperability with FORMETS systems.

- ACCS anticipates the use of gateways for data forwarding (message standard translation), trusted secure interfaces between cooperating ADP systems to control access to data, and physical interconnection of different communication systems.
- A connection-oriented virtual call protocol has been proposed for ACCS, rather than a connectionless (or datagram) protocol, as the basis for packet switched services. Virtual call services are widely used in civil networks; they can result in more efficient transmission because of significantly lower packet overheads, and they can simplify network management. An issue is whether virtual call would provide adequate flow control under stress conditions. Limited use of a connectionless service may also be required.

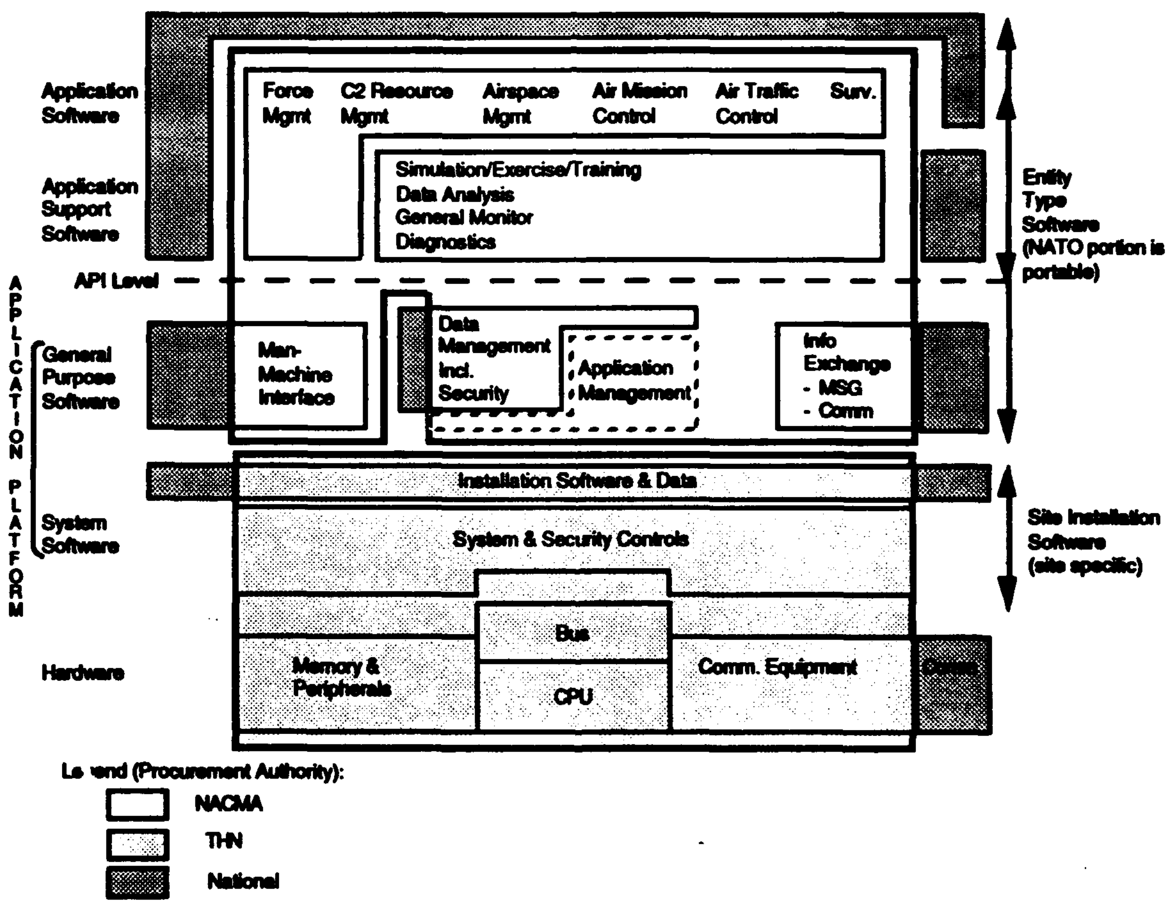
In June 1993, NACMA developed a set of views on portability, defined in NATO as "the ability of a component to operate with identical functionality in dissimilar environments," or, in other words, as a software quality factor expressing the ease with which software products may be transferred to various hardware and software environments. The concerns are with the constraints on ACCS software architecture and standards, portability testing and verification, cost, and guidelines and methods to ensure achievement of portability. One issue is whether the boundary of portable software should be at the level of general-purpose software (so that the human-machine interface or information exchange interface is portable on many different operating systems) or at the application/application support software level (so that applications are expected to run under different operating systems for many hardware platforms, relying on services offered by general-purpose software). These groups of software are shown as layers in the ACCS System Architecture (Figure 23). The term THN refers to the territorial host nation. [Ref. NACMA 1993a; Vicini 1994]

The ACCS software architecture has the following elements of application support software: simulation, exercise, training, generalized monitor, data analysis, and diagnostics. The major ACCS functions and elements of application software are the following [Ref. NACMA 1992, 1993a, and 1993b]:

- Force management (FM)—planning, tasking, and weapon/mission preparation with the goal of timely and effective C2 for the employment of air resources. ADP support is provided to facilitate force employment, option generation, and evolution. Weapon/mission preparation involves performance of air base, surface-to-air missile (SAM), and short-range air defense (SHORAD) management, as well as basic mission planning and dissemination of appropriate orders.
- Command and control resources management (C2RM)—comprises activities associated with the employment and use of the ACCS resources, including their disposition, availability, and direct logistic support. Resources include equipment such as sensors, communications, and ADP, as well as personnel and supporting services. The goal of C2RM is to enable the commander to continuously evaluate the C2 situation in order to plan, implement, and control all arrangements required to

support operations of own assets in real time and minimize interference between own C2 resources.

- Airspace Management (ASM)—plans, implements, and manages the use of airspace to ensure maximum freedom and minimum risk to own air assets.
- Air Mission Control (AMC)—directs offensive, defensive, or support missions to accomplish objectives. It includes threat warning and avoidance, vectoring for refueling operations or target attack, and safe passage through defended friendly airspace. An unambiguous air picture (recognized air picture or RAP) is necessary for performing this function.
- Air Traffic Control (ATC)—plans and controls the use of airspace, including the processes involved in maximizing traffic flow (military and civil) while ensuring safe separation and minimizing interference to friendly air operations.
- Surveillance—detects, tracks, and identifies air objects in each area of responsibility and compiles the RAP.



Source: [NACMA 1993a].

Figure 23. ACCS System Architecture

To provide a standard framework and ensure portability, NACMA intends to provide a set of standard profiles—suites of base standards together with identification of chosen classes, subsets, options, and parameters for the base standards—to its bidders. The framework recommended for these profiles is the POSIX Open System Environment (OSE) Reference Model (P1003.0) [Ref. IEEE 1992], which is a conceptual framework that provides a context for user

requirements and standards specification and a set of information system building blocks with associated interfaces, services, protocols, and data formats. NACMA is also incorporating into its recommendations the guidance provided by the Ada Implementation Subgroup (AISG) of the NACISC's Information System Working Group (ISWG) on the *NATO OSE Reference Model*, September 1993, and the ISWG *Software Standards Study*. The draft recommendations include use of a POSIX-compliant operating system, Ada, SWL, and OSF/Motif. The recommendations also address application programming interfaces (APIs) as described in the POSIX OSE. [NACMA 1993a; Vicini 1994]

18.4 Battlefield Information Collection and Exploitation Systems (BICES)

The Battlefield Information Collection and Exploitation Systems (BICES) will provide intelligence support to NATO commanders. Initially, BICES was to be a homogeneous system in all NATO nations and ACE headquarters to cover Warsaw Pact surface forces and activities. BICES today will be heterogeneous national systems that are interoperable through agreed NATO standards for cooperative intelligence in all areas for own nation, multinational coalitions, and NATO in peace, crisis, and war. From the beginning, BICES has consisted of the following three segments [SHAPE 1994]:

- Higher national segment [Chairman of Defense (CHOD)/MOD national intelligence centers and sources]
- NATO segment (NATO commands in ACE)
- Lower national segment [combat forces and systems below the principal subordinate command (PSC) level].

The BICES Team was formed to focus on national segments for BICES. The BICES Team will create tailored, unique, and specific options and recommendations for each nation in national portfolios. The BICES Pilot Study (BPS) focuses specifically on the NATO segment of BICES and the provision of BICES capabilities as an integrated element of the ACE ACCIS. Results of the BPS are due in 1995 and will contain recommendations for a near-term solution—termed the Evolutionary BICES Capability (pre-ACE ACCIS)—as well as integration into ACE ACCIS. User requirements for the ACE segment of BICES are completed: *ACE Intelligence Baselines*, 1990; and *BICES Baseline Document*, 1992. Two national gateways have been designated as part of BICES: the US Linked Operations-Intelligence Centers Europe (LOCE, also known as Limited Operational Capability-Europe) and the German Joint Analysis System Military Intelligence (JASMIN).

Among the approaches being considered for BICES are a common database and a data dictionary, whose scope and content are to be determined. NATO OSI standards from ISO and ITU-TS will be used unless they cannot meet the BICES requirements. BICES must also conform to the *NATO TCIS Transition Strategy*.

The BICES evolutionary test environment (BETE) is being developed during 1993-1997. An initial step is specification of a common LAN to provide connectivity among the nations. Provisions in the LAN standards are being made for such interfaces as PC-type asynchronous, TCP/IP, circuit-switched or packet-switched data networks, and X.25. In some cases a CISCO router will be used. Both the User Agent and Mail Gateway (CC:MAIL/X.400) and the X.400 Message Transfer Agent and Mail Gateway (X.400/SMTP) will be available. Database exchanges will initially be indirect exchanges using message or file transfer. Message exchange may be by electronic mail (unformatted messages) or AD 80-50 formatted messages. Initially, X.400:1988

will be adopted. Eventually, ADatP-3 message exchange (1995) and X.400:1992 (1997) will be supported. Graphics, imagery, and other information transfers will be supported by several types of file exchange: FTAM, FTP, CC:MAIL, or X.400. In the latter part of the evolutionary development proposed by the BICES Team for national system interoperability, direct database exchange is planned (the database standards have not been selected but may include SQL, RDA, and TP). While the early BICES capabilities support limited on-line data exchange during exercises and message/file exchange within a heterogeneous environment, the evolution will be toward indirect data exchange between heterogeneous intelligence database systems and finally supporting interactive data exchange within the BICES distributed intelligence database system. [Ref. SHAPE 1994]

A December 1993 paper [Lambert 1993] by the BICES Team noted a number of data modelling activities related to intelligence. STC has completed the draft of a three-volume report (STC TN 443) on the *ACE Data Model*. Volume I contains the initial data model developed by the ACE SD&IC; Volume II provides detailed descriptions of intelligence resource requirements (primarily orders of battle) from ACE source documents; and Volume III describes the logical structure, data elements, keys, and domains for the ACE Data Model. This work was conducted in support of BPS and provided to the BPS contractor for further data modelling work. In a related STC effort, an investigation was conducted to explore alternative approaches to database-to-database transfer by bulk load and batch updates, and a common information transfer format (ITF) was recommended. The concept was that each nation would be responsible for translation between the nation's internal transaction format at the ITF. The next step in this investigation would be prototyping. Finally, the BICES contractor (BICOM) is developing logical models for both the evolutionary BICES capability (EBC) and the ACE ACCIS BICES capability (ABC). This work is based on the earlier work conducted at STC and uses the Structured Analysis, Design, and Implementation of Information Systems (STRADIS) methodology and associated tools. An initial draft of the logical models was planned for early 1994. [Ref. Lambert 1994]

In January 1994, the BICES Team completed a draft *Functional Area Analysis Interoperability* [Ref. BICES 1994]. This document recommends a standards framework based on the POSIX OSE Reference Model (P1003.0) [Ref. IEEE 1992] and an initial set of information system standards. The standards address the following types of information exchange (termed information object types) [Ref. Lambert 1994]:

- Formatted message (e.g., ADatP-3 messages)
- Unstructured text (e.g., AD 80-50, human intelligence reports, intelligence briefings)
- Formatted data (e.g., database retrievals, bulk database loads, batch updates, spreadsheet data)
- Graphics (e.g., map overlays)
- Geographical information system data (e.g., terrain data, traffic data)
- Imagery [e.g., magazine-quality imagery, including stored-video camera (SVC) images)
- Compound objects (e.g., mixed-media documents with text and graphics)
- Digital voice (e.g., briefings, intelligence situation reports)
- Video [e.g., video teleconferencing (VTC), reconnaissance films].

These requirements may be addressed in four ways. An *information distribution mode* provides for the transfer of information from a source system to one or more destination systems,

performed on a scheduled or periodic basis or the occurrence of some external event. A *stimulated information transfer* involves an interaction between the source system and a single destination system, in which the destination system initiates the interaction. The *query-response transaction mode* allows a user to perform on-line, interactive access to information stored in a database; the information may be structured or unstructured (e.g., a text file). Finally, the informal exchange supports transactions between users that has no direct effect on stored information (e.g., electronic mail, voice mail).

A BICES Reference Model has been developed with platform services aligned with the POSIX OSE Reference Model. The applicable services and standards are defined in three forms: recommended (an international standard and an adequate number of COTS products exist); emerging (de jure national, regional, or draft international standards); and interim (de facto standards from academia or industry widely adopted and available in COTS products). The framework of the BICES Reference Model and the initial draft of the recommended standards is provided in Table 62. It should be noted that this early draft requires refinement, further market analysis, experimentation (e.g., BETE Tests 1.1 and 1.2 in 1994) and coordination with the nations before becoming stable. It is presented to show the breadth of standards identified for BICES.

18.5 NATO Maritime Operational Intelligence Support (NMOS)

The NATO Maritime Operational Intelligence Support (NMOS) will also provide intelligence support for the ACE ACCIS. NMOS provides the naval surface and subsurface picture for NATO. NMOS is a joint project under SACLANT and SHAPE. The only standards identified for NMOS that are not part of the NATO Common Interface Standards are additional STANAG 5500 (ADatP-3) messages [Ref. NMICC 1989]. The Military Committee approved the Tri-MNC concept for NMOS early in 1987. [Ref. NATO MC 1987]

18.6 Quadrilateral Interoperability Programme (QIP)

The Quadrilateral Interoperability Programme is an initiative originally of four nations—France, Germany, United Kingdom, and United States—to develop and implement, for the short term, an interface through which the four national tactical land ACCISs [respectively, Systeme Informatique de Commandement des Forces Terrestres[109] (SICF), Heeres-Fuehrungsinformationssystem fur die rechnergestuetzte Operations-fuehrung in Staeben[110] (HEROS), WAVELL, and Maneuver Control System (MCS)] can interoperate. Software development for the national systems has been completed, and an interoperability demonstration was successfully conducted in May 1990 near Ingolstadt, Germany. [Ref. ADSIA 1988a] Meetings were held in June and July of 1990 to explore options for fielding initiatives based on the Quadrilateral Interoperability Programme standards. Italy has recently joined the QIP, using its STACCON army tactical CCIS.

109 Information System for Command of Ground Forces (SICF), France.

110 Army Command and Control Information System for the Computer Assisted Conduct of Operations within Staffs (HEROS), Germany.

Table 62. BICES Reference Model and Information System Standards

System Service Areas	Interim Standards	Emerging Standards	Recommended Standards
Application Software			
Intelligence-specific applications			
Support applications			
Office automation			
Word processing	Word Perfect, Microsoft Word		
Spreadsheet	Excel, LOTUS		
Graphics	Powerpoint		
Integrated office automation and E-Mail	Microsoft Works, Aster*X, BBN Slate		
Text search			
Electronic mail	CC:MAIL		
Electronic chatter (1)			
Message handling	MMHS 2000		MMHS (STANAG 4406)
GIS applications software	Map Info		
Image processing			
Data transformation (2)			
Data analysis (3)			
Systems Software			
Operating systems	MS DOS, UNIX SVID, Windows NT, OS/2		
Database management systems	dBASE IV, Sybase, Oracle		
Human Computer Interface Services			
Graphical user interface	Microsoft Windows, Presentation Manager, OSF/Motif (4)	POSIX 1201.1 (Toolkit), COSE GUI (4)	
Window system	FIPS Pub 158 (X11R3)	FIPS Pub 158 (X11R35)	
Style guide		POSIX 1201.2	
Terminal emulation	X-Windows plus node specifics (e.g., IBM CICS)		
Security		POSIX 1003.6 (Security Interface)	
Data Management Services			
Data definition language	Vendor-specific SQL, dBASE IV DDL	SQL2, SQL3	SQL (ISO 9075:1989)
Data manipulation language	Vendor-specific SQL	SQL2, SQL3	SQL (ISO 9075:1989)
Data element dictionary	MIIDS/IDB	AIntP-3	
Data structures	MIIDS/IDB	AIntP-3	
Remote database access		RDA, SAG	
Resource definition		IRDS	
Security			
Information Exchange Services			
Text data	ASCII		ISO 646
Graphics	TIFF		CGM
Map graphics	VPF, DIGEST	RGPF	
Map products	DMA Products, CIA WDB II		
Symbol definition			STANAG 2019
Imagery	JPEG, NITF	IPI/IIF	
Video	NTSC, PAL	MPEG, HDDI	
Formatted messages	AD 80-50	ADatP-3	STANAG 2022
Documents	WKS and WK1, EDI (FIPS 161), ANSI X12		ODA/ODL/ODIF, SGML/SDIF, EDIFACT
Database information formats	MIIDS/IDBTF, MIIDS/IDBEF	AIntP-3/ITF, AIntP-3/EXT	
Security			

Table 62. (Cont'd)

Multimedia Services			
Graphics			
Two-dimensional graphics	GKS, PHIGS	PEX	
Three-dimensional graphics	GKS-3D, PHIGS	PEX	
Imagery		IPI	
Security			
Network Services			
Network applications			
Electronic mail	SMTP	POSIX 1224.1	ITU-TS X.400
File transfer	FTP, NFS, KERMIT, ZModem	POSIX 1238.1	FTAM
Directory	DNS, OSF XDS (DCE)	POSIX 1224.2	ITU-TS X.500
Terminal access	Telnet	VT	
Remote procedure call	OSF RPC (DCE)	ISO 11578 (RPC), POSIX 1003.12	
Transaction processing		XA TP (X/Open), ISO 10026 (TP)	
Network protocol suites	Internet (TCP/IP)	US GOSIP, UK GOSIP, NOSIP	
End-to-end services			
Transport/network services	TCP, IP		OSI TP0-4
Data link/physical services	IEEE 802.3, LAPD (ISDN), FDDI, X.25, Ethernet		
Network management	SNMP		
Security		ISO 11577 (NLSP), ISO 10736 (TLSP)	
Operating System Services			
Kernel	IEEE P1003.1, FIPS 151-2, XPG4	XPG-compliant POSIX	
Commands and utilities	XPG4, IEEE P1003.2	XPG-compliant POSIX	
System management	IEEE P1003.7		
Security	TCSEC (Orange Book)		
Software Development Environment			
Programming languages	Ada, C	Ada-9X, C++	
Software engineering support		PCTE	

Notes (1) Electronic chatter: direct terminal-user to terminal-user conversation.
(2) Data transformation: transforms source data (e.g., text, graphics, photographs, images, analog data) into digital data that can be processed by the computer.
(3) Data analysis: supports functions such as linear analysis, regression analysis, curve fitting, and trend analysis.
(4) Includes Window Manager, Toolkit, and Style Guide; excludes Window System.

Requirements. The Quadrilateral Tactical Interface Requirements (QTIR) document [Ref. QIC 1988] expresses the basic requirements. The Quadrilateral Technical Interface Design Plan (QTIDP) [Ref. QIC 1988a] specifies, for the gateway, the technical interface based on the ISO/ITU-TS OSI Reference Model. The operational requirements specify for information representation the use of formatted messages as described in STANAG 5621 Edition 2 and in accordance with ADatP-3 (STANAG 5500) specifications. The specifications for the common international interface between national gateways are provided in the QTIDP by annexes describing each of the seven layers with options and parameters derived from ISO/ITU-TS standards in order to meet the specific military requirements (e.g., naming, addressing, priority, sensitivity, size of messages, and segmenting).

Management. The December 1993 Quadrilateral Interoperability Programme Management Plan (QIPMP) [Ref. QIPMP 1993] provides management guidance for the QIP,

describes the management organization and procedures, and defines national responsibilities. The QIPMP identifies the following organization units for executing the QIP Programme and their roles:

- Quadrilateral Interface Committee (consisting of the program managers of the national CCISs participating in the QIP)—defining overall strategy for the program and making similar policy decisions; resolving decisions on issues passed from other boards; and developing the QIPMP
- Configuration Control Board (CCB)—drafting the Quadrilateral Configuration Management Plan (QCMP); and maintaining all QIP documentation in accordance with the configuration control procedures of the QCMP
- Planning and Execution Board (PEB)—planning and coordinating the program development schedule with the program test/field evaluation schedule; managing program execution; conducting tests, demonstrations, and exercises as required; collecting and publishing test data; and drafting the Quadrilateral Test and Evaluation Master Plan.
- Operational Working Group—providing tactical and operational advice to other working groups and boards as required; proposing information exchange requirements (IERs) for C2 of multinational formations on the basis of NATO interoperability standards; evaluating message text formats used by the QIP from a tactical point of view; and evaluating and further developing employment concepts for a QIP gateway
- Procedure Working Group—providing advice and content of NATO agreed messages and procedures for implementation of operational requirements concerning deployment and operation of gateways; analyzing NATO procedural interoperability standards designated to be used in the QIP; specifying and clarifying open details to achieve common implementation; and identifying necessary changes to NATO procedural interoperability standards and preparing change proposals to ADSIA and/or the Military Agency for Standardization.
- Exercise Coordinator's Working Group—preparing exercise plans; managing and coordinating pre-exercise activities; conducting the exercises; collecting and analyzing exercise data; and preparing an Exercise Report.

Standards and Profiles. Standards specified in the QTIDP are identified in Table 63. Specifications of Layers 1 through 5 are closely related to ISO standards. Layer 6 (presentation) is a null layer. Layer 7 specifies message handling functionality based on the ITU-TS X.400 (MHS-84) standards for the subset of service elements provided by the P1 and P2 protocols and the service elements provided by Reliable Transfer Service (RTS), as defined by ISO 9066-2, and integrated with the Association Control Service Element (ACSE, ISO 8649 and ISO 8650) that provide support for other application entities. The QTDMP [Ref. QIC 1988b] specifies a plan for interface testing and interoperability testing before performing the 1990 demonstration. Most of the interoperability parameters are specified by the options, classes, and system parameters selected from ISO/ITU-TS standards; some of the other interoperability parameters are defined in accordance with military requirements defined for messages in the QTIR.

A preliminary review has shown that all standards, stacks, and options for the Quadrilateral Interoperability Programme that are also relevant to ATCCIS have been identified in earlier chapters of this working paper. In addition, a separate analysis [Ref. Ford 1987] has been performed that identifies a large number of interoperability parameters and provides their values.

Table 63. Standards for Quadrilateral Interoperability Program

Layer	References for Standards
7. Application	ISO 8649-1988 (ACSE) ISO 8650-1988 (ACSE) ITU-TS X.400, X.401, X.408, X.409, X.411, X.420 DIS 9066.1, 9066.2 (Reliable Transfer) DIS 8824 (ASN.1) DIS 8825 (ASN.1 Basic Encoding Rules) IS 646, IS 6937 (Coded Character Sets)
6. Presentation (Null Layer)	DIS 8822-1985 DIS 8823-1985
5. Session	DIS 8326-1984 DIS 8327-1984
4. Transport	DIS 8072-1984 DIS 8073-1984
3. Network	ISO 8208-1985 (X.25 PLP) DP 8348 (CONS) DP 8472 (Network Convergence Protocol) DIS 8648-1985 (Internal Organization Network Layer) DP 8878-1984 (X.25 CONS) ITU-TS X.25-1984 STANAG 4214 (Internal Routing) STANAG 5046 (Communications Directory)
2. Data Link	ISO 7776-1985 (HDLC LAPB) DIS 8885-1985 ISO 3309 (HDLC Frame Structure) ISO 4335 (HDLC Procedures)
1. Physical	ISO TR 7477-1985 DIS 8481-1985 ISO/TC97/SC6 N3473 (DP 10022) ISO 4903 ITU-TS V.3, V.10, V.11, V.28 ITU-TS X.21, X.24, X.25 ITU-TS X.27 (EIA/RS-422-A)

Note: The table shows the status of standards at the time the QTIDP was specified.

18.7 Standard Automated Message Interface for NATO's ACCISs (STAMINA)

This summarizes the results of a review of the specifications for STAMINA. [Ref. NACISA 1988] STAMINA is being developed by an Interface Working Group of NATO Communications and Information Systems Agency (NACISA) to be used as a standard interface for passing information among ACCISs. Initial demonstrations are planned for the Central Region ACCIS and three target systems: the Allied Command Baltic Approaches Command and Control Information System (ACBA CCIS), the Central Region Alternate War Headquarters CCIS (CR AWHQ CCIS), and the Allied Tactical Operations Centre CCIS (ATOC CCIS, also known as the EIFEL Follow-On). STAMINA is planned to be used for such interfaces as [Ref. STAMINA 1990a]:

- Central Region (CR) ACCIS to UKAIR ACCIS and to EIFEL (ATOC)
- SHAPE to CR Primary War Headquarters (HQ) and to CR Alternative War HQ (AWHQ)
- ACBA CCIS to CR ACCIS and to EIFEL (ATOC).
- Various interfaces at SHAPE HQ.

STAMINA now consists of two separate transport profiles and an X.400-oriented application profile. The transport profiles support (1) X.25 packet switched networks for use in CR ACE and (2) permanent analog circuits for point-to-point interfaces using dedicated analog

circuits. (A third transport profile, switched analog circuits for use with the NATO IVSN analog voice network, has recently been deleted, as there have been no interest shown in implementing this aspect of STAMINA.)

The entire STAMINA profile for MHS-84 has been adopted by TSGCE SG9 as an intercept profile for the *NTIS Transition Strategy*. [Ref. TSGCE 1989d]

Requirements for the Quadrilateral Interoperability Programme and STAMINA overlap, but it is not clear at this time if they will converge. Generally, STAMINA attempts to provide military features (e.g., four levels of precedence and NATO classifications) as "extensions" in Layer 7.[111] Further, STAMINA provides three transport protocols (using Class 0 and Class 2), whereas the QTIDP provides just one (using Class 2). [Ref. ADSIA 1988a]

18.7.1 STAMINA Application Profile

The STAMINA Version 4 application profile for message handling is a modification of ITU-TS X.400(MHS)-1984. Eighteen military features were added; these features are identified in Table 64. STAMINA messages are free text and text formatted according to the ADatP-3 specification. [Ref. ADatP-3 1986a]

Table 64. Military Features Added to the STAMINA Specification

	Military Feature	Description
1.	Extended Authorization Info	Date and time officially authorized
2.	Subject Indicator Code	Eight subject codes for distribution information
3.	Primary Precedence	Grades of delivery (e.g., urgent, normal) for primary recipient
4.	Copy Precedence	Grades of delivery for copy recipient
5.	Security Classification	Five classifications (e.g., NATO UNCLASSIFIED)
6.	Security Category	E.g., ATOMAL, EYES ONLY
7.	Originator Identifier	Originating organizational unit message reference
8.	Address List Indication	Address list type and identifier; on origination conveys multi-destination delivery; on receipt, forwarding action
9.	Clear Indication	Transmitted without any security classification
10.	Codress Message Indicator	Indicates a codress encrypted message
11.	Corrections	Corrections are required in body of text
12.	Exempted Address	Exempted name(s) from accompanying address list
13.	Handling Instructions	Handling instructions accompany the message
14.	Message Instructions	Message instructions accompany the message
15.	Message Type	Distinguish between normal and exercise traffic
16.	Other Recipient Indicator	Identifies other recipient(s) also intended to receive message
17.	Pilot Forwarded	Used in forwarding a message
18.	Security Policy Identifier	Identifies a security policy

111 STAMINA leaves the commercial P1 and P2 sublayers unmodified and defines new service elements as extensions to P2; the QTIDP redefines both P1 and P2.

The application profile has two types of user access:

- Private Message Handling Service (MHS) Access: UA and MTA, Private Management Domain (PRMD) to PRMD, A/3211 (based[112] on ITU-TS X.400-1984 and ISO 8327)
- Military Private MHS Access: UA and MTA, PRMD to PRMD, A/3211(M) (based on ITU-TS X.400-1984, ISO 8327, ACP 117, and ACP 127).

The A/3211 application profile is the X.400 MHS, in which the Application Layer (Layer 7) has three sublayers: User Agent Layer defined by X.420, Message Transfer Layer defined by X.411, and Reliable Transfer Server defined by X.410. The A/3211 Presentation Layer (Layer 6) is defined by ISO 8823 (based on X.410), and the Session Layer (Layer 5) is defined by ISO 8327 (based on X.410).

STAMINA applications profile and the Quadrilateral Profile (QP) are both military versions of ITU-TS X.400(MHS)-1984. The QP is being developed and used by four command and control system programs in FR, GE, UK and US. The QP has a single transport profile based on X.25. To understand some of the essential differences between STAMINA and QP, note that Layer 7 of X.400-1984 consists of the User Agent (UA), the Message Transfer Agent (MTA), and the Reliable Transfer Agent (RTA). The RTA serves as the liaison with the Session Layer protocols (in X.400-1984, the Presentation Layer is a null layer; i.e., there is no layer 6, so Layer 7 liaises directly with Layer 5). Both the UA and MTA use peer (e.g., UA-to-UA) protocols to communicate to distant UAs and MTAs. The peer protocol for the UA is the Interpersonal Messaging Protocol (P2), while the peer protocol for MTA-to-MTA communication is the Message Transfer Protocol (P1). Thus, P1 defines the relaying of messages among MTAs, while P2 defines the service elements of the interpersonal messages exchanged by UAs. The STAMINA profile provides military features by extending P2 (using a "superset" approach), permitting these features to be mapped into similar commercial features in the P1 protocol without affecting lower layer protocols, whereas the QP changed both P1 and P2 in such a way that the changes affected services in lower protocol layers as well.

18.7.2 STAMINA Transport Profiles

STAMINA includes selection of ITU-TS and ISO standards—along with allowable options and parameters—necessary to attain interoperability among the end systems. STAMINA is based on profiles defined in the SPAG User's Guide. [Ref. SPAG 1987] The STAMINA transport profiles are:

- Permanent Telephonic Circuit Providing Connection-Oriented Network Service, T/21(M)
- Telephonic Switched Circuits Providing Connection-Oriented Network Service, T/22(M)
- Permanent Access to Packet Switched Data Network (PSDN), OSI Connection-Mode Services, T/312(M)

Table 65 identifies the standards specified for the STAMINA transport profiles. The current standard for STAMINA is Version 4.0, April 1990. [Ref. STAMINA 1990]

---

112 STAMINA Version 3.0 [Ref. 27] also cites "ISO 8322" for T/3211 and T/3211(M), but this standard does not exist.

Table 65. Standards for STAMINA Transport Profiles

Layer	Transport Profiles T/21(M)	 T/22(M) T/312(M)	 T/312,
4. Transport	ISO 8072 ISO 8073[a]	ISO 8072 ISO 8073[a]	ISO 8072 ISO 8073[a]
3. Network	ISO 8348 ISO 8208 ISO 8878 STANAG 4214 STANAG 5046 ITU-TS V.25 ITU-TS V.25bis	ISO 8348 ISO 8208 ISO 8878 STANAG 4214 STANAG 5046	ISO 8348 ISO 8208 ISO 8878 STANAG 4214 STANAG 5046
2. Data Link	ISO 7776[b] ITU-TS V.25 ITU-TS V.25bis	ISO 7776[b]	ISO 7776[b]
1. Physical	ITU-TS V.24 ITU-TS V.11 ISO 2110 ISO 4902 ITU-TS V.25bis MIL-STD-188C	ITU-TS V.24 ITU-TS V.11 ISO 2110 ITU-TS V.25 ISO 4903 MIL-STD-188C ITU-TS X.21bis	ITU-TS X.21 ITU-TS V.11 ISO 2110 ISO 4902 MIL-STD-188C

[a] Class 0 (Simple) and Class 2 (Multiplexing) are mandatory; Class 4 (Error Detection and Recovery) is optional.

[b] Options 2 and 8 of ISO 7809 (Balanced Asynchronous Class) are mandatory; Option 10 may be included under bilateral agreement.

18.7.3 STAMINA Development Activities

One current activity is addressing the need to add functionality required to support relays between X.400 and ACP-127 message domains, as recommended by TSGCE and recommended by the *NATO C3 Architecture* and the *NATO C3 Master Plan*. In addition, STAMINA is building a database of the interoperability parameters (e.g., speeds for communications lines) chosen by implementors of STAMINA specifications. Some parameters must be identical for interoperability and others must fall within certain ranges. The database will also track some parameters that do not affect interoperability.

A conformance test suite has been developed, and a file transfer functional profile (based on FTAM) has been defined. A new transport profile is being developed for digital circuit switch connections for communications supporting the SHAPE and CR Mobile Alternate War HQ. The current STAMINA application profile will be implemented in the STC testbed.

The Configuration Management Board (CMB) for STAMINA has agreed [Ref. US 1988] to add the additional military features to the X.400 specification, making it identical to MMHS(84). Version 4.0 of STAMINA should be reviewed for such compliance. The CMB has decided to omit one part of STAMINA, the Transport Profile for Analog Circuit Switch, which was seen as high risk and for which no interest has been expressed from implementors. There are plans to develop another transport profile for STAMINA for digital circuit switched communications. NACISA is interested in studying the compatibility of STAMINA with the 1988 standards, with an orientation to migrate toward a 1988 base or, alternatively, define an interface module between the 1984- and 1988-based systems.

Some STAMINA parameters are left to be determined by the implementors of an interface, and some of these must be the same on both ends of the interface. NACISA has developed a

database in which to record the parameters used on all STAMINA implementations. NACISA has begun to develop a new project called the Automatic Message Processing System (AMPS). It appears at this early stage that it will have two aims [Ref. NACISA 1990]:

- To provide individual ACE HQs with automated message handling capability internal to each HQ for generation of outgoing messages and to provide the processing of incoming messages. Initially, the messages will be transmitted via the existing TARE system using TARE-unique protocols. Where possible, the internal processing will be based on X.400 oriented systems.
- To use the AMPS at each HQ as the platform for the eventual replacement of the TARE with an X.400 oriented network.

The interface standards to be used with ACE are expected to migrate from TARE-unique protocols via STAMINA/MMHS-84, through MMHS-88, and eventually to X.400 commercial standards.

An ACE ACCIS Integrated Testbed is planned to support NATO CCIS development efforts, e.g., the BICES Pilot Study (BPS) effort, with NACISA serving as the host nation and STC providing scientific expertise and the home of one of the testbed nodes.

18.8 Other NATO Initiatives Using Open Standards

This section briefly identifies a number of other NATO initiatives using or planning to use open standards in their development and procurement.

18.8.1 NATO Initial Data Transfer Service (NIDTS) Program

The NATO Initial Data Transfer Service (NIDTS) Program will establish a NATO packet switched network interconnecting NATO organizational subnetworks and selected national networks. It will be used to link intelligence centers operating LOCE. Phase I has begun, in which NIDTS will acquire the routing elements and network management components to provide interconnectivity among 12 locations. Related to the NIDTS program is the cryptographic equipment for packet switching (CEPAS) Program, which will acquire the packet encryption devices for the NIDTS network. NACISA has stated that the NIDTS network will most likely be based on TCP/IP protocols. [Ref. Messina 1993]

18.8.2 NATO Internet Architecture

A presentation on the NATO Internet Architecture was provided by Mr. Tony Whyman (McCallum Whyman Associates Ltd, UK) to the October 1992 meeting of TSGCE SG9/WG5.

18.8.3 Communications System/Network Interoperability (CNSI)

CNSI is a collaborative activity between Canada, France, Germany, the Netherlands, the United Kingdom, and the United States, with participation by SHAPE Technical Centre. The objective of the project is to demonstrate the technical feasibility of military communications systems internetworking, using an OSI-based architecture in accordance with STANAG 4250. It is intended that this demonstration should provide the background experience to permit NATO to move forward with the definition and ratification of STANAGs for interoperable systems. The project is governed by the terms of the Memorandum of Understanding on CNSI concluded between the participating nations in December 1991. [Ref. Bot 1993] Project responsibility now resides in the CNSI Steering Committee and its subordinate body, the Technical Coordination Group (TCG). The TCG will develop detailed project plans. Documents of CNSI will be marked "in confidence," and with distribution limited to participating nations unless specifically approved by the CNSI Steering Committee. [Ref. Gee 1991]

The emphasis of this 3-year effort is not on developing standards but rather to demonstrate the operational utility of internetworking using enhanced OSI profiles with military features, specifically demonstration and evaluation of multi-media communications extending from the West Coast of the United States to the center of the European continent. [Ref. Rigden 1991]

The CNSI Project will provide a demonstration of the NATO OSI concepts when applied to a variety of applications supported by a diversity of transmission media and an evaluation of the associated protocols and standards that will have to be used to fulfill the operational tests. Operational benefits expected to accrue from this work are the following [Ref. Bot 1993]:

- Enhanced survivability of military command, control, and communications networks, including anti-jam protection
- Effective interchange of information among the heterogeneous C2 systems
- Improved evolutionary growth potential for C2 and communications systems
- More effective use of communication capacity.

CNSI will support both voice and data communications. Data communications in general will be packet switched, while voice communications will be circuit switched as a real-time synchronous bit stream. No packetized voice will be used. Voice and data communications will share the CNSI transmission media, and voice circuits will be established on demand. The set-up of voice calls will be done in a packet-switched fashion using the CNSI lower layer protocol stack. Non-voice communications will be multi-priority. Voice circuits will be assigned a high priority level within the data priority scheme. [Ref. Bot 1993]

The CNSI project plans a demonstration in 1994 for linking subnetworks of countries across long haul multimedia networks supporting multiple modes (voice, data, images). Use of HF ground-wave and sky-wave, VHF, UHF line of sight, UHF SATCOM, SHF SATCOM, and land lines is planned. According to the MOU [Ref. TSGCE 1990j], WG3 will (1) ensure that the work will be closely related to the recommendations, standards, and draft STANAGs of all groups under SG9; (2) provide both feedback into the STANAG development process and practical experience on the implementation of OSI protocols on military bearer systems; (3) provide reports on the demonstration results and performance to SG9; and (4) based on demonstration results, recommend to SG9 the adoption of promising system concepts for different operational applications. An outline of the work areas originally considered for the CNSI statement of work is given in Table 66.

The CNSI demonstration entails the creation of a connectionless internet comprising multiple subnetworks of different media. The inter networking protocol will be CLNP, (ISO 8473). The messaging application, based on X.400, will make use of Class 4 COTS (ISO 8073). The Tactical Data Generator will use CLTP (ISO 8602), enhanced to offer multicasting. [Ref. Bot 1993]

Very limited information on the progress of CNSI is generally available, since CNSI policy only allows information to be released to participating nations. This policy has severely restricted the potential liaison with interested groups in TSGCE SG9, specifically the AHWG on Security and WG5.

Table 66. Proposed Work Areas for CNSI

1.	System Concepts and Testing
a.	System demonstration architecture
b.	Testing program
2.	Applications and Services
a.	Database exchange
b.	Security
c.	Voice
d.	Messaging
3.	Multinetwork Management and Protocols
a.	Multimedia routing
b.	Enhanced OSI protocols
4.	Communications Media and Systems
a.	Long haul HF
b.	Satellite communications (SATCOM) SHF
c.	SATCOM UHF
d.	VHF
e.	UHF LOS
f.	EHF ELOS
g.	EUROCOM
h.	ISDN/GSM.

Source: *Proposed Terms of Reference for WG3*, TSGCE SG9 WG3, October 1991, NATO UNCLASSIFIED.

18.9 Analyses Supporting Military Application of Open Standards and Standards Deficiencies

This section briefly provides extracts from analyses conducted by the nations on the potential military use and suitability of open standards and on deficiencies observed in the civil standards. Most of these extracts are from the *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993,* STC Symposium Proceedings SP-10, June 1993. The analyses are arranged into several subject areas.

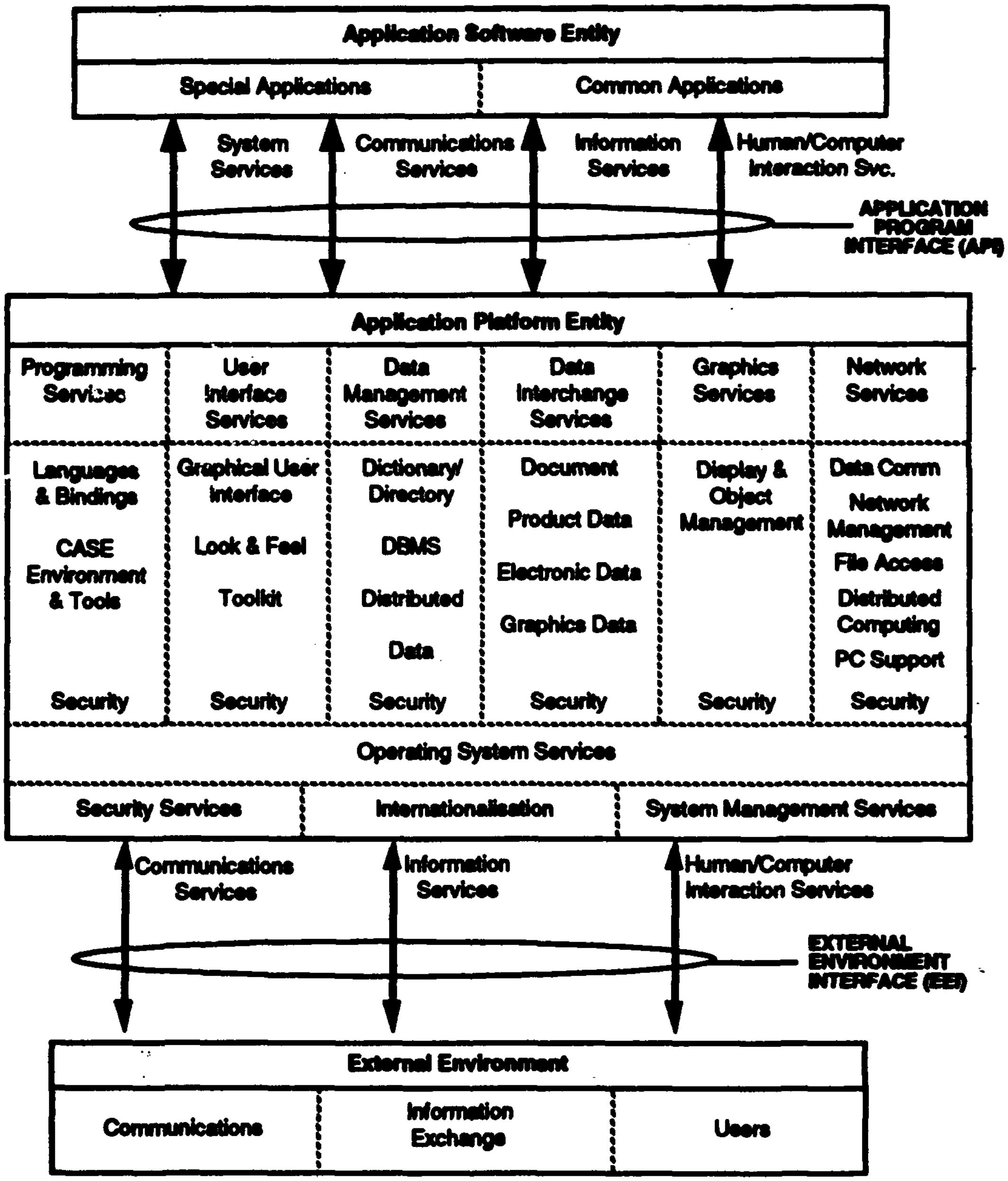
18.9.1 NATO Standardization

18.9.1.1 NATO OSE Reference Model

In July 1993, the Information Systems Working Group (ISWG) of the NACISC distributed the NATO OSE Reference Model (RM) to the NACISC for approval. The OSE RM is nearly identical to the POSIX OSE RM (P1003.0) [Ref. IEEE 1992] and is shown in Figure 24. Comparison with TRM of Figure 1 in Chapter 1 shows that instead of using a third dimension to specify security, internationalization, and system management, the NATO OSE RM (as well as the POSIX OSE RM) identifies these service areas in boxes surrounding the operating system services. In addition, the NATO OSE RM (and POSIX OSE RM) do not yet address distributed computing services as an eleventh service area. Identification of the elements of the services areas is very similar but not identical among these OSE RMs.

18.9.1.2 NATO OSE Baseline Architectural Principles

The NATO OSE baseline architectural principles are statements of preferred architectural direction or practice focused on how NATO wants to use information system technology in the long term. The objective is to establish a context for standards-based architectural modelling and help translate standards-related criteria into a language that NATO managers can understand. These principles, listed in Table 67, are arranged in four categories: information technology policy matters, life-cycle management, application management, and technology management. [Ref. NATO OSE 1993]



Source: [NATO OSE 1993].

Figure 24. NATO OSE Reference Model

Table 67. NATO OSE Baseline Architectural Principles

Information Technology Policy Matters
• All future NATO MIS and CCIS systems will be required to be compliant with the agreed NATO Open System Environment (NATO OSE).
• All future software-intensive NATO MISs and CCISs will be procured in an evolutionary manner.
• Systems will be implemented such that maximum advantage will be taken of standard (commercial and NATO owned) components throughout NATO.
• Choices of technology will be based on vendor independent standards where available and implementable.
• The order of precedence for the use of standards will be: first, STANAGs based on international standards; international standards; then commercial or industry standards; and finally STANAGs- or NATO-specific standards that are not based on international or commercial standards.
• NATO policy will ensure that information systems and COTS components comply with adopted standards.
• Standardization of data definitions and their implementation, access, and communication is required across NATO.
• Implementation of Security measures and contingency plans will be derived from a NATO common security policy.
• Security products that could act as a barrier to open systems will be avoided.
Life-Cycle Management
• NATO systems are to be developed in such a way that they recognize the need for future changes to functional and technology requirements.
• Software will be developed using NATO adopted standard methods.
• NATO will exploit the utilization of reusable components wherever and whenever possible.
• Application software will be developed so that it can be reused in similar application domains across NATO
• Where possible and economically feasible, COTS hardware and software components will be procured.
• The NATO architecture and implemented systems must address the management of all forms of information (data, text, sound, video, and image) in an integrated manner.
• Security features will have similar characteristics and a consistent interface across application domains.
Application Management
• The NATO OSE will provide for distributed system scaleability.
• Applications will be implemented in a common environment that is independent of the underlying technology.
• Applications will conform to a common user interface that is adaptable and extendible to particular user requirements.
• The NATO OSE will enable application software portability at least at the Source Code Level.
• The NATO OSE will enable application software and application platform interoperability.
Technology Management
• The NATO OSE will accommodate existing, imminent, and new information technology standards.
• NATO OSE-compliant systems will be scaleable to platforms of varying power and implementation complexity.
• The user processing environment will be decentralized as much as possible allowing the user community a measure of control over their own computing resources.
• Workstations will be the primary access and delivery platform for applications and data.
• NATO will use a common network environment using NATO OSE adopted standards to interconnect workstations, computers, and communicating devices.
• Communicating devices must interface to the common network environment through a standard set of protocols and interfaces.

Source: [NATO OSE 1993].

18.9.1.3 NATO Standardization Strategy

A long-term strategy for standardization activities in NATO must take into account the following observations [Ref. White 1993]:

- The definition of requirements for new systems is often vague, incomplete, or absent, so standards practitioners must make informed estimates of the future needs.
- In a rapidly changing world where military involvement can take many forms—with mixed forces thinly spread—it is essential to provide easily deployed interoperable, user friendly command and control.

- In all but mobile narrow-bandwidth applications, examination of military features is increasingly revealing the adequacy of emergent civil sector standards. Security and management remain focal points for military concern.
- In such circumstances, key distribution for secure systems becomes a critical impediment and indicates the need for the use of asymmetric public key systems, at least for start-up purposes.
- Civil sector standards are being driven by technology. NATO needs to determine which areas of this new technology it is likely to require for C3I.

A synthesis of these issues can be achieved by adopting the Open Distributed Processing five-view-points model, which defines a system from the viewpoints of enterprise, information, computation, engineering, and technology. The strategy drawn from this approach would focus on the following [Ref. White 1993]:

- Interactions are actually needed by NATO [enterprise]
- Application/information is exchanged [information]
- Processing is required [computational]
- Physical system will be needed [engineering]
- Technologies should be anticipated [technology].

18.9.2 Coexistence and Convergence of Internet and OSI Standards

Requirements. An open system strategy for TCP/IP and other Internet protocols should include its evolution towards ISO, which requires that the use of non-OSI compliant applications (several of which have been developed for TCP-IP) be restrained. Some in presenting the standards program do not admit this pre-OSI offering, but TCP/IP has evolved because of user market forces. There is no use in ISO open system purists pretending it is not there–US GOSIP includes it. The bottom line is that there are thousands of users and more than 200 vendors offering TCP/IP products. [Ref. White 1993; Lynch 1991]

Convergence.[113] Since IP only provides the minimum functions required to transport datagrams from sources to destinations, TCP provides the functions to provide reliable process-to-process communications. The functions provided by TCP are similar to those supported by TP. Recognizing these similarities, the National Research Council recommended in 1985 that the US DoD transition to TP4. [Ref. Wells 1993]

The US DoD, like other committed users to ISO standards, has been frustrated by a lack of available ISO transport-profile products. Therefore it continues to use TCP/IP with plans for transition to TP4/CLNP. Other military and civil users are also plagued by a lack of ISO transport-profile implementations. They are also turning to TCP/IP products to solve their current computer networking problems.

One of the major factors for the growth of TCP/IP implementations around the world, and especially in Europe, has been the need for LAN/WAN internetworking. User sites today are characterized by one or more LANs used to interconnect PCs, workstations, and servers. LANs are connected to a variety of WAN network types including X.36, Frame Relay, SMDS, and point-to-point links. The only protocol family currently available to support the interconnection of such a large variety of network types is TCP/IP.

---

113 This section is based on extracts from [Wells 1993].

Recognizing a future need for interworking between Frame Relay and B-ISDN networks, ITU-TS depicts scenarios where TCP/IP is used in the end systems, in which appropriate relays are provided. In addition, the NATO C3 Architecture includes LAN/WAN internetworking with the use of TCP/IP stacks. The Director General NACISA has issued a memorandum [Ref. DGNACISA 1992] stating that all NACISA program managers will specify the mandatory use of TP4/CLNP to ensure interoperability across a variety of subnetworks.

The development of "real" ISO-based products for the LAN/WAN internetwork environment has been significantly delayed for two reasons: (1) the connectionless versus connection-oriented debate, and (2) the ISO process for developing standards. COTS products for LANs and LAN/WAN internetworking are based on connectionless oriented protocols that are either de facto standards such as IP or proprietary protocols such as Internetwork Packet Exchange (IPX). The TCP/IP suite also includes routing and management (i.e., Simple Network Management Protocol) protocols. Although most governments, major corporations, and NATO have established policies for the use of ISO/ITU-TS standards, this has to be viewed as a long term goal. Near-term implementations have to consider the availability of COTS products. For example, the European Procurement Handbook for Open Systems (EPHOS) specifies the use of ISO standards. However, it recognizes the real world need to consider non-OSI stacks (e.g., TCP/IP) for near term LAN/WAN interconnections; and the eventual migration from this non-OSI environment to an OSI one.

NATO should adopt the same policy as EPHOS and major corporations for LAN/WAN environments. It should no longer debate the pros and cons of connection- and connectionless-oriented network services, but should use proven COTS products and develop a migration path to an OSI environment based upon TP4/CLNP.

18.9.3 Architectural Issues

Distributed Systems.[114] A client-server model provides an efficient and effective environment in which a user accesses distributed computing resources and storage facilities through user friendly interfaces. A client-server model basically consists of workstations such as personal computers (PCs) through which the users request the computing services, servers that provide the computing services and data storage and a LAN that transmits data between workstations, workstations and servers, and servers. Figure 25 shows the elements of the client-server model.

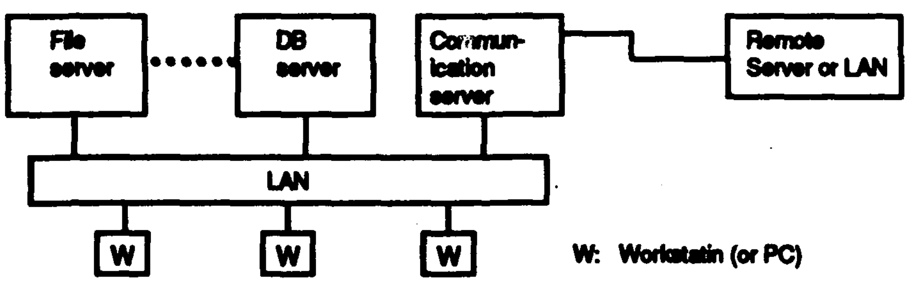
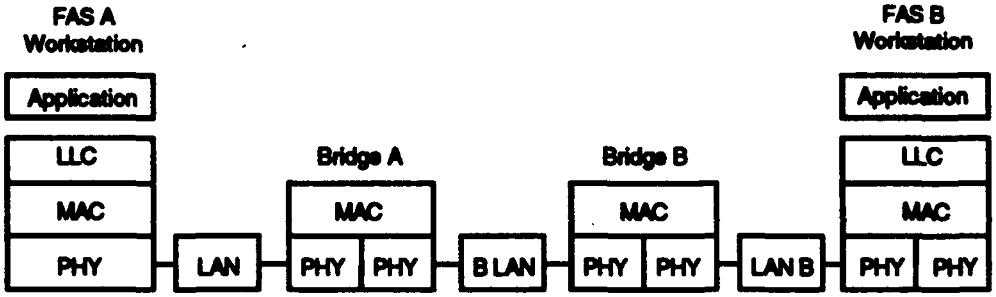


Figure 25. Elements of Client-Server Model

114 This section is based on extracts from [Gungor 1993].

The functionality provided by a client-server architecture depends on the functions provided by its servers. Servers are computing elements (PCs, minicomputers, microcomputers, or mainframes) equipped with the required software to provide a set of predefined services to the users upon their request. This model enables distribution of computing services between server(s) and workstations and offers an efficient and flexible solution in meeting the needs of work group environments. The client-server model proposed could involve several specialized and general purpose servers that may be called on to provide a variety of services (such as database operations, message handling, image processing, etc.).

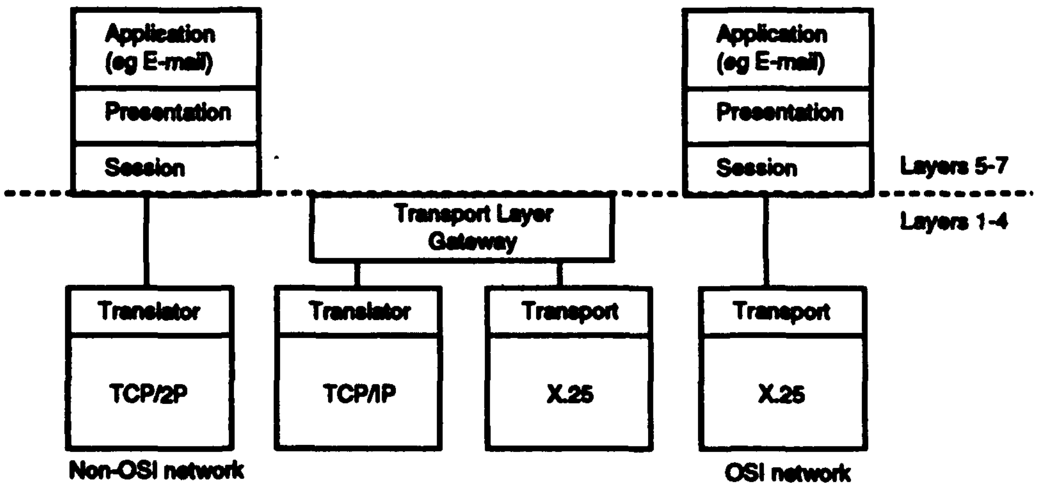
To minimize the number of the gateways required in the NATO C3 Architecture and to enable the sharing of computing resources common to all or several Forward Area Systems (FASs), a backbone system is proposed. The backbone system is a client-server based subsystem consisting of a LAN, servers providing services common to several or all FASs, elements to enable the data exchange with other IS nodes, and workstations to be used for system management purposes. To differentiate the LAN of the backbone system from the LANs of the FASs it will be referred to as "backbone LAN" (B LAN). Connecting the LANs of FASs to the backbone LAN will be sufficient to establish full connectivity within the IS node (Figures 26-28). To interconnect six FASs, there will be a need for six gateways.



Key: LLC: Logical Link Control PHY: Physical
MAC: Medium Access Control BLAN: Backbone LAN

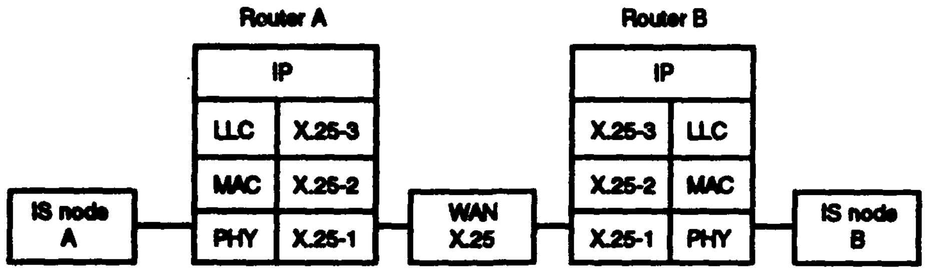
Source: [Gagnor 1993, p. 205].

Figure 26. Connection of Two FASs Through the Backbone System



Source: [Gagnor 1993, p. 206].

Figure 27. Transport Layer Gateway Between TCP/IP and OSI



Source: [Gagnor 1993, p. 207].

Figure 28. Two IS Nodes Interconnected Through Two Routers and Wide Area X.25 Network

Connectionless and Connection-Oriented Modes.[115] The ISO standards necessary for subnetwork independent CLNS networking exist but have not been validated in large scale networks. ISO support for CONS networking is subnetwork dependent and limited to a single subnetwork. Consequently, commercial networking products available in the near future are more likely to support the CLNS than the CONS. With the NATO and member nations' policy of COTS procurement wherever possible, the technical capabilities of the two modes for meeting the military requirements need to be determined. This paper discusses two military requirements impacted by the network service mode, namely security and network availability.

The CLNS security mechanisms are less capable than those available with the CONS, and high assurance of end-to-end connectionless security is not likely to be available in the near future. While connection-mode network security is adequate for all identified requirements, the adequacy of connectionless network security depends on the class of application.

Connection mode networks manage congestion through allocation of resources when the connection is set up and by invoking data flow control. Connectionless networks, which are prone to congestion, discard data and rely on users backing off, which is inconsistent with the military requirements for network availability and an acceptable quality of service.

It is recommended that NATO support research into large scale validation of the connectionless-mode protocols and the development and validation of subnetwork independent connection-mode protocols. The ability of the CLNS to adequately meet the military requirements of security and network availability under operational conditions needs to be determined. Research in both network service modes reduces the future risk to NATO in the provision of networks to meet military requirements under operational conditions.

It is necessary to put into context the work ongoing in the ISO community addressing the issue of interworking between the CLNS and the CONS. ISO TR 10172 describes a Transport Relay Interworking Functional Unit, which enables interworking between the CONS and the CLNS by relaying between the two in the transport layer. Although the Transport Relay may help to achieve interworking, it does not remove the need for communicating end systems to operate in the same network service mode if there is an end-to-end requirement for functionality provided by one mode and not the other.

CLNP includes several Subnetwork Dependent Convergence Functions (SNDCFs) that provide for the use of various different subnetworks, while the subnetwork independent part of

115 This section is based on extracts from [Gungor 1993].

CLNP provides an identical network service to the transport layer regardless of the actual type of subnetwork the system is attached to. CLNP must be implemented in every ES needing to interoperate using the CLNS. In contrast to the ISO standards support for the CLNS, no subnetwork independent protocol has been developed by ISO to provide the OSI CONS. Currently, the CONS is provided by the subnetwork dependent protocol specified in ISO 8878, which maps on to the services provided by X.25. The CONS is delivered to the transport layer by ISO 8878, which can only run over a single X.25 subnetwork. An X.25 subnetwork, from the OSI perspective, may actually be multiple X.25 networks interconnected using X.75, which is a non-OSI interface protocol between X.25 networks.

No subnetwork independent protocol or supporting routing procedures have been developed for the CONS. The only ISO support of connection mode routing at present is limited to the application of ISO 10030 within a specific subnetwork. This protocol describes the Subnetwork Address Resolution Entity (SNARE), which enables an ES to query a subnetwork-specific database. By so doing, the ES can determine where on the subnetwork it can find a given destination. This protocol is the most that can be currently specified to support CONS routing until a CONS subnetwork independent protocol has been developed.

In the connectionless mode, NLSP and TCS are specified to support CLNP, and they provide security mechanisms to support the network layer security services available with the CLNS. In most CLNS networking scenarios, NLSP or TCS will not be at the top of the network layer in order to provide functionality above and below NLSP or TCS to support segmentation and re-assembly on the trusted and untrusted sides of NLSP or TCS. Consequently, to achieve secure end-to-end networking, trusted intermediate systems, which perform trusted relaying and routing of protected traffic, are required. These are difficult to develop and are unlikely to be commercially available in the foreseeable future.

It has been suggested that the shortcomings in the provision of CLNS security can be overcome through the use of transport layer functionality. For example, security services may be provided by ISO 10736, the Transport Layer Security Protocol (TLSP), or by additional local management functionality to link the ISO 8073 Transport Class 4 (TP4) and the NLSP mechanisms. Both methods rely on the functions of the TP4 mechanisms for their operation. Therefore, if rigorous military security is to be applied to the connectionless mode, TP4 implementations must be built to the required assurance levels in addition to NLSP or TLSP. Delivery of highly assured TP4 mechanisms is believed to be beyond the current and foreseeable security evaluation techniques for high assurance.

Much work has been performed by the military community on network layer security for both connection- and connectionless-mode networks. Within the constraints of the modes, excellent technical solutions have been developed. This work has influenced the development of NLSP through the national standards bodies. The end-to-end provision of the CONS has been assumed in the development of security protocols to provide security services to meet the NATO requirements. The connectionless mode security services are always less capable than the connection-mode security services, particularly for the provision of integrity. Security in the connection-mode environment is adequately provided by NLSP with the TCS enhancements, but in the connectionless environment the available security services may not be adequate for some classes of application. Since the security services required must be defined in accordance with the total system security requirement, for many applications sufficiently secure communications may be achieved using either mode.

Connection Orientation.[116] Table 68 summaries the chief features of CLNS and CONS.

The end-to-end provision of the CONS has been assumed in the development of the NATO TCS, which, through the NATO member nations, has influenced the development of ISO NLSP. The connectionless security services are less capable than the connection-mode security services, particularly for the provision of integrity, so the connectionless mode may be inadequate for some classes of application.

Table 68. Salient Features of the CLNS and CONS

	CLNS	CONS
Interoperability	Not interoperable with CONS	Not interoperable with CLNS
Networking Standards	Full set exists; needs validation	Need further development and validation
Security Services	Adequacy depends on requirement; Trusted ISs required for end-to-end security	Adequate for all known requirements; Trusted ISs not required for end-to-end security
Route Allocation	On each packet end to end	At connection set-up and localized re-routing after route failure
Error Recovery	End to end recovery traffic	Localized recovery traffic
Packet Overheads	Higher	Lower
Packet Size	Unpredictable segmentation within network, reducing performance and promoting congestion	At connection set-up size negotiated down to maximum that can be delivered by all subnetworks
Congestion Control	Catastrophic congestion possible, even in benign environment; discards data, relies on user's backing off	Predictably controlled through resource allocation and flow control

Source: [Turner 1993].

For end-to-end security in the connectionless mode, trusted ISs are required; these are not likely to be available in the foreseeable future. Trusted ISs are not required for end-to-end-security in the connection mode. Highly assured transport layer security functionality to supplement CLNS network layer security functionality is not likely to be available for the foreseeable future.

Connectionless networks are more vulnerable to congestion than connection-mode networks because in connectionless networks, management actions such as error recovery and re-routing are end-to-end actions leading to greater traffic for all subnetworks. In connection-mode networks, error recovery and re-routing mechanisms are localized.

Packet overheads are higher in connectionless networks than connection-mode subnetworks. Spontaneous segmentation in connectionless networks gives rise to unpredictable traffic generation and degradation of performance due to increased switching overheads and increased probability of congestion. In connection-mode networks, the packet size is negotiated down at connection set-up to the maximum size that can be delivered by the traversed subnetworks.

Relief of congestion in connectionless networks relies on discarding data and network user's backing off, which is inconsistent with the military requirements of network availability and acceptable quality of service. Catastrophic congestion is a known problem of connectionless

116 This section is based on excerpts from [Turner 1993].

networks, typically due to retransmissions of discarded packets. Connection-mode networks manage congestion through resource assignment when the connection is set up, with data flow control invoked as necessary to provide reliable end-to-end data transfer.

Multicasting. Table 69 summarizes multicasting requirements.

Table 69. Summary of Multicasting Services Required by Application

Services/ Application	Group Open/Closed, Determinate/ Indeterminate, Static/Dynamic, Size	Communication 1-way/2-way/ n-way, Fixed/Single/ Unrestricted	Transmission Reliable/ Unreliable, Synchronized/ Unsynchronized	Data Rate, Throughput, Delay
Distributed Simulation	Closed, Determinate, Dynamic, 100-10,000 members	n-way, unrestricted	unreliable or reliable; Unsynch	High rates, Real-time or near real-time
Tactical Messaging	Closed, Determinate, Dynamic, 2-10 members	n-way, unrestricted	reliable, Unsynch.	some real-time constraints
Database Updates	Determinate, Static, 75-200 members	2-way, single transmitter	reliable, Synch.	non-real-time
Image Distribution	Closed, Determinate, Dynamic, 2-100 members	2-way, single transmitter	reliable, Unsynch.	Image size up to 100 Mb.
Naval platforms	Closed, Determinate, Static, 20 members	1-way, single transmitter	reliable or unreliable; Unsynch.	near real-time or real-time.
Computer-Supported Cooperative Work	Closed, Determinate, Dynamic, 3-200 members	2-way, single transmitter	reliable (text), unreliable (video), Unsynch.	near-real-time

Source: [Turner 1993].

18.9.4 OSI Issues

Quality of Service. Early work in QoS tended to focus on a set of general qualities of service, using functional groupings such as quality of addressing, quality of message (i.e., integrity), quality of timeliness, quality of confidentiality, and quality of cost, although later work in NATO suggested that interoperability, quantity, frequency, services, security, "quality," timeliness, availability, and survivability were the specific qualities of interest to the military. [Ref. Sluman 1993]

Military Messaging: ACP-127 and ACP-123. Apart from standards for common application service elements (CASE) provided by ISO, and the range of civil applications with obvious military use (FAX, voice, video, etc.), messaging is an established military application, although it has been evolved in a fairly ad hoc way over many years. The NATO messaging standard ACP-127 is used by over 70 nations. ACP-123 is a future messaging standard being developed by Australia, New Zealand, Canada, the United Kingdom, and the United States ACP-123 is intended to be a complete stand-alone definition, including protocols, for message exchange. These standards are also being developed to cater use over limited capability HF channels and over a busy packet switched network. The messaging element is based on X.400, but is not formally aligned with the SG9 program, which contains a series of X.400 bases MMHS standards and includes provision for ACP-127. [Ref. White 1993]

Analyses, Simulations, and Demonstrations for Use of X.400.[117] An analysis was conducted in 1991 of a typical X.400 message converted from an ACP-127 message

117 This section is based on excerpts from [Bryant 1993].

to examine header overhead. For a seven-recipient message, over 3 kbytes of overhead were required to generate the X.400 envelope and header, whereas an equivalent ACP-127 message has an overhead of 0.5 kbytes. Substantial contributors to the X.400 overhead were originator/recipient addresses, trace information, security features, and encoding techniques. [Ref. McArthur 1991]

A traffic simulation was conducted in 1992 by MITRE for DISA. The recommendation from that study was that a full OSI stack can be deployed in those tactical systems having more bandwidth and processing capable systems [such as the Mobile Subscriber Equipment (MSE)], but that in general OSI is not recommended for use in tactical radio systems that must support near-real-time delivery requirements. [Ref. MITRE 1993]

Participating in the third Strategic-Tactical Data Network (STDN-3) demonstration, DISA evaluated X.400 for strategic-tactical interoperability and concluded that X.400 electronic mail can support that interoperability. X.400 appeared suitable from a performance aspect for relatively high-bandwidth tactical networks such as the US Army Tactical Packet Network (TPN), which includes MSE. There was no substantial difference in performance between X.400 and its current alternative, SMTP. No conclusions were reached for radio links. An overall result was a basis for optimism for military message's being able to extend from the strategic community well into the tactical community without the drawbacks of specialized gateways.

Evaluation of ASN.1 Enhancements for Tactical Data Communications.[118] A significant portion of any ASN.1 encoded PDU is occupied by overhead bits such as tag values, length octets, and pad bits. For small message sizes (i.e., fewer than 10,340 octets), such as those used for tactical C3, the amount of overhead is at least 11 percent. For 5,120-octet messages, the overhead figure is approximately 30 percent, and for a 2,048-octet message (not uncommon for tactical applications) the encoding overhead exceeds 60 percent. Note that encoding overhead is exceeded by X.400 overhead, which adds typically 200-300 percent overhead to user-supplied message bodies fewer than 10,240 octets in size [Ref. Bonatti 1993].

Several techniques can be used to minimize encoding overhead, including tag and length octet omission, intelligent ordering of fields in the abstract syntax, nesting omission, numeric range adjusting, and bit alignment. These are addressed by the following proposals, now being incorporated into encoding standards [Ref. Bonatti 1993]:

- Packed encoding rules (PER). PER (DIS 8825-2.2) provides a more compact form of tag-length-value encoding that is faster to process than the BER. PER uses octet-aligned tag-length-value encoding in which the type and length identifiers are frequently omitted. It also uses tag omission, length-code omission, and numeric range adjustment techniques to minimize encoding overhead.
- Distinguished encoding rules (DER). DER (DIS 8825-3) uses a tag-length-value format similar to BER but eliminates the many alternative encodings that are possible with BER. The DER is useful in cases, such as cryptography, where independently generated encodings must be identical.
- Lightweight encoding rules (LWER). LWER (DIS 8825-2.2/WDAM1) does not use tag-length-value encoding but an alternative that is faster to process because the encodings generated are similar to commonly used local storage formats. LWER is designed to maximize processing speed of the encoder at the expense of flexibility, extensibility, and compactness. It does so by defining the transfer syntax to match the

118 This section is based on excerpts from [Bonatti 1993].

local representation format as closely as possible through the use of six new transfer syntaxes that cover a broad spectrum of representation formats. These syntaxes define rules with varying word sizes and octet ordering schemes. Since LWER will generally increase encoding overhead significantly, it is primarily useful in high-speed applications where bandwidth is plentiful or where processing resources are extremely limited. The latter case might apply to some tactical scenarios, such as hand-held-device satellite communication (SATCOM).

- Minimum basic encoding rules (MBER). MBER [Ref. Blum 1990] was proposed by the civil aeronautical community, whose aim is similar to PER, but with a more aggressive approach. A unique aspect of MBER is employment of bit alignment to further reduce the size of resulting encodings. This feature requires a new ALIGN constraint for the ASN.1 notation, which would allow abstract syntax developers to specify particular alignment requirements (e.g., octet alignment) for any field. Many of the MBER features have been used in PER, but, because MBER offers significantly lower encoding overhead than PER, its proposals may need formal consideration. MBER has not yet been submitted to ISO as a separate standard.

OSI Management. SG9 has concluded that there are no special features required for military managed objects within the ISO managed objects model of management. Indeed, SG9 has yet to definitively establish any uniquely military object. The main area of concern is whether management is sufficiently secure. Security features available to all applications may suffice, provided there is an understanding of the QoS and security parameters for management. [Ref. White 1993]

Network Management.[119] Network management standards are targeted at the data communications area. In the telecommunications area there are additional requirements that can be met by a supplementary set of standards. These are collectively known as Telecommunication Management Network (TMN) and are described in a number of ITU-TS recommendations (M.3xxx series). Furthermore, there are ISDN-related recommendations for testing at the network interface level (Q.94x series). It is expected that the *NOSIP Strategy* over time will be expanded to encompass all relevant communication profiles by including the standards that are relevant for telecommunications management. [Ref. Christiansen 1993]

Within the NATO community there are existing systems and equipment that will be prohibitively expensive to adapt to international standards. Among these are switching systems (i.e., IVSN), backbone systems (i.e. SATCOM and NTTS) and special equipment (e.g., cryptographic units). These systems implement their own proprietary protocols and services. They cannot be discarded in the near-term future and they will have to be an integrated part of the future system. The challenge is to decide how much to invest in accessing them from a management point of view. Some standards do anticipate non-standard systems by allowing for proxies (within OSI) or mediation devices (within TMN). These implement a standards-compliant-object as front-end for the non-compliant element. The number of these front-ends is expected to decrease over time. This is expected to happen when the non-standard devices are replaced by standard compliant resources.

119 This section is based on excerpts from [Christiansen 1993].

18.9.5 ISDN Issues

Use of ISDNs.[120] After a period of field trails in the late 1980s, public ISDN services became commercially available in most West-European countries between 1989 and 1992. In Eire, Greece, and Turkey, public ISDN will start in 1993. Currently, most European countries offer public ISDN services in the major cities using a national version for user-network signaling. However, all the major European public telecommunication service providers agreed on a memorandum of understanding (MOU) about providing ISDN access and ISDN services in a harmonized way. The MOU will be implemented in three steps. Step 1 ensures that ISDN will be available in all European countries in a basic harmonized version by the end of 1993. Although the services of Step 1 are very limited, it will provide a European-wide standardized user-network protocol that is the precondition for terminal portability within Europe. In Step 2 some bearer and supplementary services will be added by the end of 1994. The most important services of Step 2 are probably the packet switched services within the B- and D-channels. After completion of Step 3 the whole set of agreed services will be available. There is no fixed schedule for Step 3, but it is expected to be implemented by the end of 1995.

The situation in North America is more difficult than in Europe because of independent local telecommunication service providers. After a period of non-compatible ISDN islands "ISDN 1" was developed as a nationwide ISDN service providing standardized Basic Access. The interfaces and protocols are implemented according to standards from ANSI and NIST. Unfortunately, the North American ISDN standards are slightly different from the European ISDN standards. ISDN 1 was presented nationwide at the end of 1992 in the "Transatlantic ISDN Project. The next step will be "ISDN 2," which will also support Primary Rate Accesses.

If the basic infrastructure is in place, ISDN can be used for a variety of services and applications such as:

(a) Interconnecting LANs through routers at much higher data rates than are available via analog telephone networks.

(b) Providing ISDN teleservices (e.g., telephony, video, high-speed facsimile). Teleservices can be provided stand alone or in integrated packages that will facilitate the development of multimedia applications. In the user area, teleservices can also be integrated with OSI applications such as FTAM or message handling.

(c) Relatively high-speed bearer capability for access to packet switched networks.

Bearer and teleservices can be augmented by a variety of supplementary services, such as voice and video conferences, calling line identification, closed user groups, etc., provided by the public ISDNs or by the end-systems. Multilevel precedence and preemption has been standardized by ITU-TS. Nevertheless, it is still open whether and when it will become available as a publicly available supplementary service.

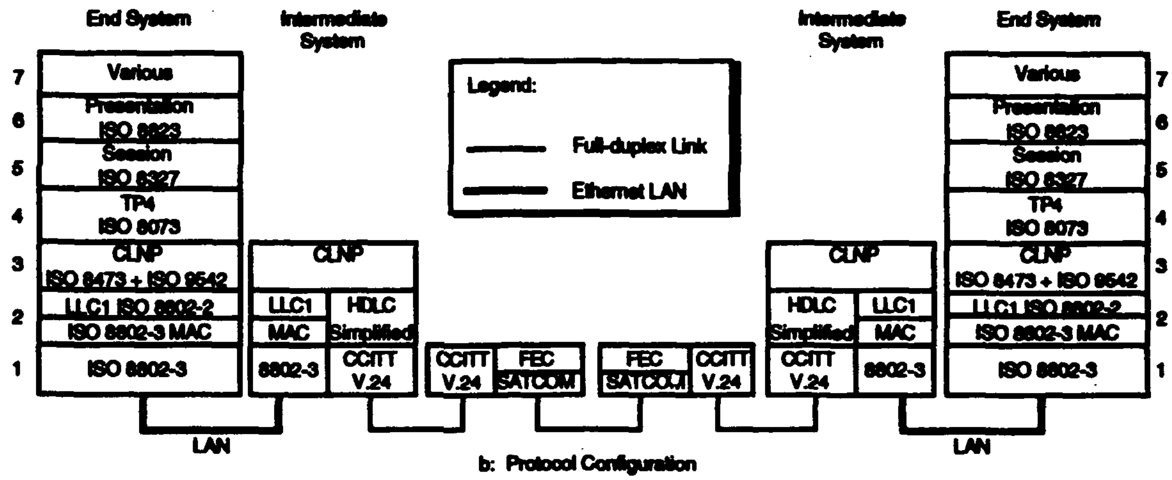
The AHWG on ISDN in TSGCE SG9 provides guidance and standards, based on civil standards developed by ITU-TS, ETSI, and ANSI, in the following areas [Ref. Stollenmayer 1993]:

- ISDN user-network interfaces and protocols
- ISDN inter-exchange signalling systems such as CCS7 and QSIG
- ISDN services such as bearer services, teleservices and supplementary services

120 This section is based on excerpts from [Stollenmeyer 1993].

- ISDN security (in liaison with the SG/9 ad hoc group on security)
- ISDN and OSI related issues
- ISDN numbering and addressing.

Use of OSI and ISDN in SATCOM.[121] It has been successfully demonstrated that SATCOM links supporting static and mobile users can be integrated into networks utilizing OSI and ISDN standards. The SATCOM link provided a bit stream service (64-2048 kbit/s) without any special protocol enhancements. The choice of protocol, protocol options, and variables is critical in achieving good performance with SATCOM links. An example scenario for use of OSI and ISDN in SATCOM is provided in Figure 29.



Source: [Hind 1993].

Figure 29. OSI End-to-End Configuration with Connectionless Network Protocol

In order to achieve the tests performed to date, several test beds were developed and interconnected at STC. As a result, the value of using rapid prototyping and integrated test beds to achieve quick results was demonstrated.

A critical aspect of achieving good throughput is the error recovery technique that must be compatible with the SATCOM delay and error characteristics; the OSI transport protocol Class 4, as implemented in the STC OSI test bed, was found to give good performance and is also tolerant to slips. In the case of low capacity noisy links, further study is required in order to identify optimum protocols, particularly where signal processing functions—such as spread spectrum and coding—introduce additional delay.

For data applications, the typical error performance of SATCOM links (10^{-5} for >99.9) is adequate to support OSI/ISDN services, assuming the use of TP4 for data applications; furthermore, two links in tandem could be utilized while achieving an acceptable throughput. The use of concatenated forward error coding (inner: convolutional/Viterbi, outer: Reed-Solomon) enables error performance of 10^{-10} to be achieved with a modest bandwidth expansion.

121 This section is based on excerpts from [Hind 1993].

18.9.6 Multimedia and Packet Radio Technology

Multimedia. XTV (X Teleconferencing and Viewing), a workstation-based collaborative computing system in the X-Window environment that allows geographically separated users to simultaneously view and manipulate shared images, documents, or programs while they communicate via audio and possibly video links. XTV is a public domain system developed by Old Dominion University and the University of North Carolina at Chapel Hill. XTV allows a conference to be created around one or more arbitrary X applications. Participants have the same view of shared applications and, by following a simple floor passing protocol, may control the shared applications. As an X-based application, it can operate in any X-based environment, on a TCP/IP network. XTV offers almost unlimited flexibility within an X-based environment because it is designed to facilitate the sharing of *any* X-based application. [Ref. Turner 1993]

In the usual model of X, the user's workstation (the server) interacts over a network with the application (the client). In XTV, the server acts as a conference master and shares the output from the application with other conference participants. A token determines which conference participant is controlling input to the application at any time. At present, XTV uses multiple TCP transmissions for the output from the conference master to the conference participants. The multiple TCP transmissions used previously for the output from the server conference chair to the many conference participants have been replaced by TP4 with extensions providing a reliable one-to-n multicast service with two-way data flow. [Ref. Turner 1993]

Packet Radio Architecture. The architecture of packet radio networks can be classified as centralized or distributed. In a centralized network, there is one central transmitter/receiver, attached to a central resource. All other nodes communicate only with the central node. Node-to-node communication is indirect, mediated by the central node. The earliest networks followed this model, and were designed primarily to provide terminal access to a central time-sharing system. In a centralized system, two radio channels are required. Individual nodes send packets to the central node on one channel, and the central node broadcasts packets on another. Since radio transmission is omnidirectional, packets transmitted by the central node are heard by all the other nodes. Thus the configuration is logically equivalent to a multipoint line with a primary and a number of secondaries. [Ref. Stallings 1991]

The first packet radio network, ALOHANET, was developed by the University of Hawaii and became operational in 1970. Its principal objective was to allow user terminals in widely scattered locations to access the university computer system. Traffic was primarily terminal-to-host, but terminal-to-terminal traffic could be routed via the central node, called the menehue (Hawaiian for "imp"). Remote units were of two types. The terminal control unit (TCU) operated with a simple half-duplex terminal and included a buffer, control logic, and transceiver. The programmable control unit (PCU) was a microprocessor-based device for terminal concentration and/or a computing station.

An increasingly common application of distributed packet radio is to provide distributed networking among personal computers, including access to centralized computing resources. In most cases these networks consist of amateur radio stations and are open to any user who conforms to the protocol used on a particular network.

Amateur packet radio networks exist in a number of areas throughout North America, and the number is growing steadily. An effort to standardize these networks has been underway since

1982, under the sponsorship of the American Radio Relay League (ARRL), which has produced a standard for a link-level protocol suitable for packet-radio networks known as AX.25.

An ARRL-type network is a distributed network, organized into clusters of stations connected by repeaters. All stations and repeaters share a single frequency for transmission and reception. The AX.25 standard does not specify the frequency to be used. Based on FCC-approved channel availability, the typical network uses the 220-MHz band, using FSK and with ALOHANET, a fixed routing scheme is used. In this case, the route to be followed is specified by the source station, as explained below. (p.336)

The most important difference between AX.25 and HDLC is in the addressing technique. In HDLC, there are two possible configurations: A point-to-point link with two stations, and a multidrop link with one primary and multiple secondaries. In either case, a single address is sufficient for the operation of the protocol.

18.9.7 Software Standards for NATO

Software Standards Study. A *Software Standards Study* was completed in March 1992 by the Information Systems Working Group (ISWG) of the NACISC.[122] This document provides substantive recommendations regarding the potential viability of adoption by NATO of standards in specific areas of software-based systems. It addresses international standardization efforts in the areas of operating systems, user interfaces, interoperability and networking, and database languages, which are believed by the ISWG to be the most beneficial to NATO in adopting an open systems approach. The survey of standards contained in the annexes of the *Software Standards Study* provides major supplementary material to the top-level information provided in this document. This is particularly true of the information the *Software Standards Study* provides on UNIX standardization (Annex A, 180 pages), graphical user interfaces (Annex B[123], 26 pages), and database query language (Annex C, 20 pages). The architecture framework for the *Software Standards Study* is shown in Figure 30.

As seen from the list of technical annexes given above, the Software Standards Study focuses on only three areas of the architectural framework shown above: UNIX and POSIX for the Platform Area; graphical user interfaces for the User Area; and database query languages for the Language Area. Interoperability, as defined in the study, is the ability of applications running on software and hardware from multiple vendors to communicate meaningfully. Interoperability and networking are treated in the study only in relation to UNIX data formats and communications protocols (currently dominated by use of TCP/IP in the UNIX market). A migration towards OSI is seen as gaining momentum.

The following are issues about the characterization of standards needed and available to support the architectural framework (Figure 30):

- The study overestimates the need and value of adopting a common operating system for NATO and poorly characterizes UNIX, which is recommended. Indeed, UNIX is cited[124] as "a typical example of an open system." Incompatibility problems among

---

122 *Software Standards Study*, AC/317(W/2)N/332, Final Draft, NATO Communications and Information Systems Committee, Information Systems Working Group, 26 March 1992, NATO UNCLASSIFIED.

123 Annex B is based on a study conducted for the Canadian Department of National Defence by APG, Inc., 30 September 1991 (Project GUI01.9102).

124 *Software Standards Study*, op. cit., Section 4.1 (p. 4).

various versions of UNIX from different vendors is noted. POSIX is claimed[125] to be a series of operating system standards that "could provide the ultimate goal of both source level and possibly object level compatibility."

- The study asserts[126] that "SUN's Network File System (NFS) for distributed file systems is a guarantee for file system interoperability" and "POSIX standardization of the tape archive utility assures interoperability of data formats among UNIX users"—such assertions seem far from the truth, given the other requirements in data management and data standardization, not to mention other aspects of transfer mechanisms and data presentation syntax that are required for interoperability.
- The need and role of application program interfaces (APIs) for portability (and interoperability) are not addressed.
- Security is only addressed by noting the growing availability of secure UNIX operating systems and certified UNIX products, with the note that computer security evaluation may be required to determine whether the integration process has created vulnerabilities not identified in the individual product evaluation.
- OSF/Motif was selected based on an analysis of 26 criteria; however, Motif and OPEN LOOK had nearly identical (within 3 percent) raw and weighted scores, and no clear rationale for choosing Motif over OPEN LOOK was given. Windows 3.0 was recommended for MS DOS platforms.

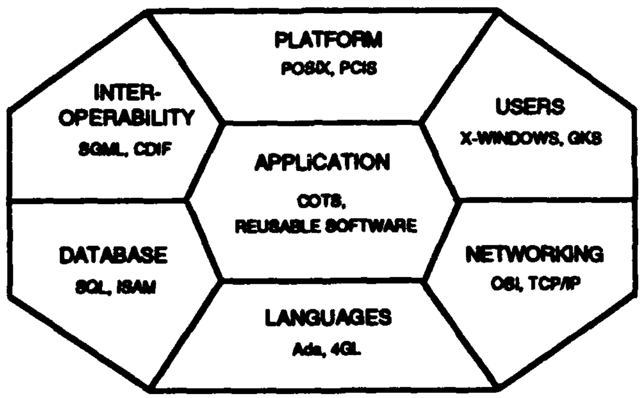


Figure 30. Architecture Framework for Software Standards Study

Among the recommendations made in the study are the following:

- NATO establish adoption criteria and procedures to allow implementation of Open System Architectures and internationally agreed standards.
- NATO adopt UNIX as the standard operating system platform for all communications and information system and management information system applications.
- NATO require that all its UNIX platforms and products are in conformance with the X/OPEN Portability Guidelines. This includes for the basic UNIX environment adherence to the following standards:
  - POSIX.1
  - Draft POSIX.2

125 *Ibid.*

126 *Software Standards Study*, op. cit., Section 4.1.2 (pp. 5-6).

- ANSI-X3.159-1989 C-Language standard (only in the exceptional circumstances where conformance to the NATO Ada policy is not possible and a waiver is granted)
- X-Window System
- ANSI SQL standard with X/OPEN-defined system dependencies.

- NATO closely monitor the evolving UNIX standardization process to ensure rapid access to the new developments.
- NATO adopt MOTIF as the standard graphical user interface.

NATO Software Standards. In March 1993, the NACISC noted the recommendations of the *Software Standards Study* cited above. Without endorsing the recommendations, the NACISC provided wide circulation of the results within NATO and the nations. [Ref. NACISC 1993e]

Software Methods and Tools Study. In July 1993, the Ada Implementation Subgroup (AISG) of the ISWG distributed three papers addressing software methods and integration, integration guidance, and development tools. This effort was an outgrowth of a project on life cycle methodology conducted during the period 1988-1991. The project reviewed the major software development and maintenance methods in general use, together with their associate automated tool support, for three classes of systems: automated management information systems, real-time embedded systems, and C3I systems. The 1993 recommendations are the following [Ref. NACISC 1993d]:

- The methods identified in the study as currently commercially viable can now be used effectively by NATO.
- In order to provide full systems life cycle support within NATO, it is necessary to assess the integration of the identified methods into a life cycle methodology.
- Adequate data now exists in order to assess and identify suitable existing full life cycle methodologies (supported by commercial tools) for potential NATO use.
- The ISWG task the AISG to develop a work program and schedule for the way ahead for ISWG consideration.

Each of the three papers provided in the 1993 study provided data and analysis of issues for integrating structured analysis (e.g., data flow diagrams) and hierarchical object-oriented design (HOOD) methods. Among the tools considered (and the nations submitting the data) were the following: Concerta (FR), IPSYS (UK), SELECT (UK), STOOD (UK), TEAMwork (US), AdaNICE (IT), EPOS (GE), and Virtual Software Factory (VSF) (DK).

18.9.8 CCISs for NATO

The paper *CCIS for NATO: Critical Factors Related to Implementation of an Open Systems Architecture* is a civil (unsolicited) contribution[127] from the Armed Forces Communications-Electronics Association (AFCEA) to NATO that contains specific recommendations on standards for use in future CCISs. Its genesis was to contribute to the ongoing debate about NATO CCISs in general and about the ACE ACCIS program (see Section 18.2) in particular. The central theme of the paper is to present the case of an open systems architecture, which is a major theme of WP 25 as well. The paper provides rationale for an open systems architecture, outlines how military features and open system attributes influence

127 The paper was prepared under the direction of senior officers of Bull, Siemens, and Digital and a review board consisting of members of AFCEA who have (or had) senior/general officer rank in NATO nations.

an architecture, presents an ACCIS Reference Model, identifies relevant open and de facto standards, and recommends a set of standards applicable for an open systems architecture for NATO CCISs.

The rationale for an open systems architecture may be summarized by the following observations made in the paper:

- Ample evidence [is] available to conclude that a similar architecture, using similar standards, could be applied for both management information systems (MISs) and CCISs.
- Security and performance requirements in particular, and to a lesser degree the functional requirements, would be key drivers for different information systems under the same architecture.
- Use of the open system architecture approach would ensure the required features of interoperability, scaleability, compatibility, and portability without impacting on other facets such as vendor neutrality, affordability, and the fulfillment of essential requirements.

The AFCEA Study suggests that there are three steps in specifying CCISs suitable for NATO (and in particular for an ACE ACCIS). First, strategic goals, generic characteristics, and system-specific characteristics are transformed into an ACCIS Reference Model, which identifies architectural elements, design characteristics, and interfaces between functional elements. Second, standards (and some "standard products") are selected for applicable functional elements in the ACCIS Reference Model to produce an ACCIS architecture. Third, additional products are selected in accordance with standards set forth in the architecture, system-specific development is performed, and system integration is conducted to produce a fieldable configuration. Note that WP 25 identifies standards for interfaces and architectural elements that would be used for the first two steps. (While all three steps will be taken in support of the ATCCIS Phase III Demonstration now planned for September 1995, it is outside the scope of ATCCIS to select products, which is a national prerogative. A single common configuration is *not* a goal for ATCCIS—a single set of standards to ensure interoperability *is* a goal of ATCCIS.)

The AFCEA Study cites the US DoD Technical Reference Model (TRM) objectives and principles[128] (similar to those of the NATO OSE shown in Table 67 above) as reasonable objectives for the ACCIS Reference Model and revises seven of the principles to provide a set of technical means for reaching the objectives.

Figure 31 presents the ACCIS Reference Model proposed for NATO in the AFCEA Study paper. It consists of five layers: hardware, operating system, common services, applications, and user interface. The common services are: interoperability services [network services and application profiles for file transfer, message transfer, remote login, remote application execution, visual display unit (VDU) conversation, distributed file system, and link message exchange]; data interchange; data management; languages; and graphics services. Details of these layers are derived from the US DoD Technical Reference Model.

Figure 32 presents the standards recommended for the ACCIS Reference Model. These standards form the recommended open system architecture for ACCISs. No standards are needed for hardware, other than the survivability and electromagnetic shielding that would be specified by existing NATO standards. For personal computing, the Intel X86 is recommended because of the

128 Apparently, Version 1 (November 1991) of the Technical Reference Model was used in the AFCEA Study.

numbers of COTS applications available. Standardization for operating systems is recommended to be built on standard interfaces between the operating system and the other layers in the ACCIS Reference Model, for which POSIX (IEEE 103.x) is identified. In addition, the X/Open Portability Guide (XPG) and the OSF Level (last release) are recommended. For personal computers, MS-DOS is recommended and the emerging standard New Technology (NT) is highlighted for close attention. The paper clearly states that no standard operating system is needed. Rather, the best platform (operating system and hardware) should be selected for the system's mission.

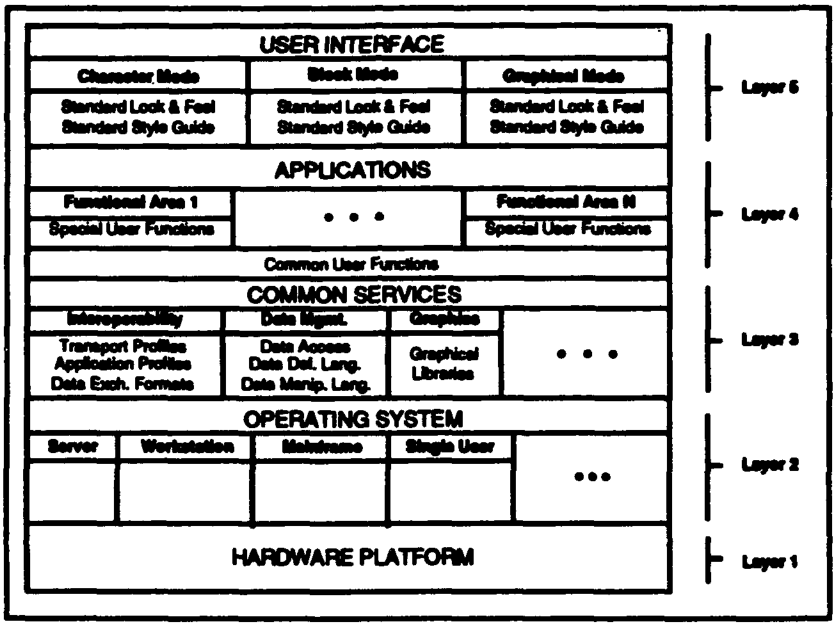


Figure 31. ACCIS Reference Model Recommended by AFCEA Study

USER INTERFACE OSF Motif (MS-Windows/NT)				
APPLICATIONS CCIS/MIS Functional Areas				
COMMON SERVICES				
Network Services	Data Interchange	Data Management	Languages	Graphics
OSI TCP/IP	ODA/ODIF SGML EDIFACT CALS	ANSI SQL (ISO 9075) (SQL2) (SQL Access)	FORTRAN-77 COBOL-85 Extended Pascal C Ada	MIT X11 (PEX) GKS PHIGS
OPERATING SYSTEM XPG3 POSIX (MS-DOS/NT)				
HARDWARE PLATFORM				
Best Suitable Hardware Platform				

Figure 32. ACCIS Reference Model Standards

The following observations are made for the ACCIS Reference Model:

- More than one operating system is to be expected for ACE ACCISs. Standardizing on one operating system for a single headquarters is seen as "highly favorable and should be pursued to the maximum extent." The AFCEA Study further suggests that a single operating system should be established for a backbone infrastructure throughout the headquarters. (In ATCCIS, it is expected that dissimilar hardware platforms may be used in a single headquarters and that more than one operating system should be supported by the architecture—selection of hardware and operating system should remain a national option, and common local area network standards should permit interoperability.)
- Users should be permitted (Remote Application Execution) to specify that an application be run on a computer other than the user's workstation but residing on the same local or wide area network. (The requirement for remote processing goes beyond Basic Interoperability—the exchange of information that preserves meaning and relationships—and is therefore not included in the ATCCIS architecture. However, remote procedure call is included in WP 25—see Section 9.11.3.5.)
- Users should be able to conduct VDU Conversations, in which a user's input on a local terminal appears as output on other terminals connected to the same local or wide area network.
- Users should be able to treat (some) remote files as if they were local files, independent of physical location on a local area network. Remote procedure calls would be used to allow separate applications to exchange data structures and commands in support of the distributed file system capability.
- Tactical digital information links (TADILs) should be capable of being exchanged across local and wide area networks. This would be used, for example, by applications that handle a recognized air picture (RAP) or a recognized sea picture (RSP).

- The need for logical (conceptual) data models is recognized for data management but is excluded from the ACCIS Reference Model.
- A single access protocol, which defines how data are returned to applications, is needed that can be used with various data definition languages (DDLs) and data manipulation languages (DMLs) for different types of file systems. Standard DDL and DML (e.g., using SQL) would mask out differences among vendor database management systems (DBMSs) and make applications independent of a particular DBMS or file system.
- Two types of distributed database models are noted in the AFCEA Study, and a recommendation is made that one should be chosen as the best basis for meeting operational requirements. (In ATCCIS, a mixed model is anticipated that combines both of the concepts noted here.)
  (1) Database replication duplicates parts of a local database to a remote site. Database replication requires a universal data model that is enforced for all database segments being replicated. Replication is triggered on updates of data elements within the segment of the database being replicated or on a periodic basis. Applications access the "copy" that is stored locally. The size and contents of segments being replicated depend on operational requirements. (In ATCCIS, this is referred to as a partitioned, partially replicated database.)
  (2) Database federation uses a distributed database system to join (or federate) physically separated database segments into a virtually seamless global database spanning all units. The size and contents of segments being federated depend on operational requirements. Database federation also depends on a universal data model that is enforced for all segments. In its pure form, there is only one instance of data (no replication). Applications requesting data from a part of the federation that is not stored locally issues a request via the networks and the data are returned via the networks.
- The applications layer of the ACCIS Reference Model isolates applications from the other layers to facilitate portability, component interchange, and reuse, as well as to allow insertion of new applications without disrupting operations. Applications exclusively use APIs offered by the common services and user interface layers (no application-to-application integration or direct data exchange).
- The user interface layer is defined using the NIST User Interface System Reference Model (see Section 5.3).

Nine selection criteria are identified and used in the AFCEA Study. These are:[129]

- Existing hardware and software (the installed base)
- Capability to provide required security features
- Availability of standards and products
- Availability of COTS products
- Capability to provide the needed functionality
- Portability
- Scaleability, enabling the same applications and software to be used on all system classes with computer-specific restrictions
- Interoperability (defined as the ability to share data and functions across networks)
- Survivability (to include real-time update of databases).

---

129 Standards selection criteria have not yet been addressed in this paper. Such criteria are the subject of a separate activity in ATCCIS (Select ATCCIS Standards and Profiles). See the *ATCCIS Phase III Work Plan* [Ref. ATCCIS 1993].

(This page is intentionally left blank)

19. NATIONAL INITIATIVES FOR MILITARY USE OF OSI STANDARDS

This chapter identifies national initiatives that make or plan to make significant use of OSI standards in military applications. Major bilateral and multilateral initiatives are discussed in the main body of this working paper; these include the Quadrilateral Interoperability Programme (Section 18.6) and STAMINA (18.7).

The primary purpose of this review of national initiatives is to identify the ways in which military features are being addressed in national systems. In some cases, there may be fully-compliant use of OSI standards. In other cases, there may be defined some extensions to the standards that could be considered by international bodies as candidates for new options to the commercial standards, so that in the time frame of ATCCIS (and other NATO CCIS projects) the military features (e.g., a secure local area network) may be specified by civil standards. On the other hand, analysis of national initiatives may lead to conclusions that some features may need to be specified as deviations from civil standards and, in these cases, the relevant STANAGs may need to have similar deviations.

National initiatives are addressed, where possible, in terms of requirements, profiles, and transition strategies that have been recommended or adopted. A short review is provided of work being done to evaluate the performance of civil standards for military applications. Several initiatives that have led to fielded operational capabilities are discussed in some detail in Appendix C

19.1 Canada

Canada is participating in the IGOSS, which will serve as the basis for Canadian (and US) GOSIP. CA GOSIP will be promulgated as the Canadian Open Systems Application Criteria (COSAC) and issued as a Treasury Board Information Technology Standard (TBITS). [Ref. IGOSS 1993]

Canada has been conducting testing to integrate various protocols on a variety of systems, including X.400 over OSI LANs, OSI applications of TCP/IP, X.500 access through Internet, and application gateways such as FTP-to-FTAM running on a SUN workstation. A demonstration capability developed by the Canadian Office of the Director General Communications and Electronics Engineering and Maintenance includes the following [Onufer 1992a]:

- OSI LAN: TP4, CLNP, ISO 8802-2, ISO 8802-3
- OSI applications over TCP/IP: X.400, X.500, FTAM, and VT
- OSI applications over X.25: X.400 and FTAM
- OSI/TCP gateways: SMTP-to-X.400, X.400-to-SMTP, FTP-to-FTAM, and FTAM-to-FTP
- TCP/IP LAN.

The Canadian Army is replacing its present tactical communications systems in the near term (1996-98 time frame) under a Tactical Command Control Communications System (TCCCS) projc :t with an integrated tactical communications system called Iris. The Iris Radio System will provide a complete family of modern CNR equipment with embedded voice and data encryption and frequency hopping capabilities in the VHF band, plus specialized AGA and combat HF radios for all vehicles and hand-carry roles. The system also includes local area systems for the headquarters, a trunk system, single-channel radio access (SCRA) facilities, a system-wide tactical message handling system (TMHS), a long-range communications system (LRCS), and a management system for both the communications system and the cryptographic material used [Ref. German 1993].

The Iris architecture includes the following [Ref. German 1993]:

- Local Area System (LAS)—the Headquarters Information Distribution System (HIDS), which is a highly modular and flexible local communication system with a common architecture to satisfy the requirements of headquarters for elements ranging from a full division to a subunit. The HIDS provides the full telephone services of the EUROCOM D/1 standard.
- Wide Area System (WAS)—a combination of the Iris trunk system, providing multichannel line-of-sight communications for voice and data; and the LRCS, providing satellite and high-power HF voice and data communications within Iris and with external systems. In the Trunk Distribution Network (TDN), the frame relay service is replaced by an ATM cell with cell-head forward error correction (FEC). Data uses the IP protocol overlaid on frame relay in the Local Distribution Network (LDN) and ATM with FEC in the TDN. Data switching is done by IP routers throughout the TDN, the LDN, and the Mobile System.
- Mobile System—a combination of the CNR suite of radios and the SCRA system that includes tactical extension nodes (TENs) to provide access to the Iris Trunk System for mobile users (packet radio is not provided, but the TMHS extends throughout Iris including CNR nets; message relaying is handled at the applications layer within the TMHS). For other than CNR use, TMHS institutes the full X.400 (1988) suite of service and offers interface to ACP-127, ACP-128, and JANAP-128-based messaging systems; to Canadian Forces MMHSs, and selected commercial MHSs through a variety of gateways. For CNR use, TMHS offers a subset of the X.400 (1988) services, together with the capability of broadcasting to all the members of a net.
- System Management and Control System (SMCS)—a combination of the Communication Management System (CMS) providing EUROCOM D/0 and OSI management facilities, and the Cryptographic Material Management System (CMMS) providing management and distribution facilities for all the key material and equipment within Iris.

19.2 Denmark

CCIS Testbed. During the period 1993-1995, the Danish Army will be developing a C2 testbed for a prototype CCIS. This work will lead to an implementation of an Army Command and Control System in 1996. The current C2 testbed, which has been on trial at HQ/Jutland Division and which will be introduced in 1994 at brigade level, consists of the following [Ref. DK MOD 1994]:

- SUN/SPARC servers and workstations
- UNIX operating system
- INGRES database management system

- Fairchild Multimap geographic information system (GIS)
- UNIPLEX.

The testbed uses SUN TCP/IP over an Ethernet LAN running at 2 Mbps and SUN PPP at 9.6 kbit/s. These are connected to the national field trunk network, the Danish EUROCOM Communication System (DEOS).

DEOS. DEOS is a EUROCOM grid-area communication system that is operational from division down to brigade and independent battalion echelons. The standards of the tactical communications network of the Danish Army (DA) are based on EUROCOM D/O and D/1 basic parameters. DEOS is a circuit-switched trunk node network (TNN) used primarily as a voice network, but it has the capability for data communications. The nodes are connected via bulk-encrypted line-of-sight connections. [Ref. DK MOD 1994]

The switches in the network can be used to interconnect the following types of subscribers and information [Ref. DK MOD 1994]:

- Analog PTT (public telephone network)
- Analog telephone subscribers (non-secure)
- Digital telephone subscribers (secure to the SECRET level)
- Facsimile (secure to the SECRET level)
- Teletype (TTY)
- Data.

The DEOS network has the following interfaces [Ref. DK MOD 1994]:

- Connection of tactical trunk nodes to NATO or national mobile tactical, fixed, or strategic networks, using multiple STANAG 5040 (analog) interfaces.
- Connection of tactical trunk nodes to the national PTT.
- Connection to a EUROCOM network via a EUROCOM gateway. For the subscribers numbering plan, DEOS uses STANAG 5046, the *NATO Military Communication Directory System.*

19.3 France

Army Tactical CCIS Systems. Army tactical CCIS systems in France are using or are projecting to use more and more components based on OSI standards. The Army is following the general recommendations of standards organizations such as AFNOR, SPAG, ITU-TS, and CEN/CENELEC (see Appendix F), and would thereby try to use, wherever possible, the products (hardware and software) built upon these standards.

One example of the implementation of OSI standards in Army tactical systems is the use of ETHERNET™ (ISO 8802.3) to link cells within a command post. In addition, tactical networks, such as RITA and RETINAT, are based on ITU-TS X.25 packet switched standards. Table 70 identifies the international OSI standards that the Army intends to use in its standardized MHS Gateway, based on QTIDP specification.

RETINAT. RETINAT is a data communications system for the French Army. The network operates 33 switches of two types (one for military districts and one for military regions). The network accommodates 1,400 synchronous and 600 asynchronous ports and supports data rates from 300 bps to 64 Kbps. The switches are interconnected with 64-Kbps trunks and use X.75 gateways for interoperability with other data networks. [Ref. Cassese 1990]

Table 70. French Army Standardized MHS Gateway

OSI Layer	International Standard	Brief Title of Standard
Application (Layer 7)	ITU-TS X.400:1984 ISO 9066/1:1987 ISO 8649:1986, ISO 8650:1986	MHS RTSE ACSE
Presentation (Layer 6)	ITU-TS X.409:1984	Abstract Syntax Notation
Session (Layer 5)	ISO 8326:1986, ISO 8327:1986	Basic Service and Protocol
Transport (Layer 4)	ISO 8072:1985, ISO 8073:1984	Class 2 Service and Protocol
Network (Layer 3)	ISO 8208:1985	Basic Service and Protocol
Data Link (Layer 2)	ISO 7776:1985	HDLC LAP B
Physical (Layer 1)	ITU-TS X.21:1984	

Source: [Romann 1992].

Real Time Transport Service (RTTS). The French MOD has developed an architecture and implementations of that architecture for a Real Time Transport Service (RTTS). GAM-T-103 is a specification for an implementation of this architecture. [Ref. GAM 1987] RTTS results from more than 15 years of experience in the design and realization of real-time data networks for military systems. RTTS provides not only data communication services but also synchronization and management services. RTTS was described at the June 1990 Military OSI Symposium at STC. [Ref. STEI 1990] The paper addressed the ISO Transport Service, real-time constraints, and a proposed real-time Transport Service. It presented the classes of service, the models used for data transfer, the connection-oriented and connectionless modes for communication services, the synchronization services, and the management services. RTTS has been proposed in draft STANAG 4254 (Annex E) as the basis for defining real-time services for NATO CCISs.

There are two current releases of the Real Time Transfer Protocol specification:

- GAM-T-103B, available in French only, is interfaced with a data link service near to the MAC service to support the STANAG 1553 Military Bus (with the STANAG 391) extension). GAM-T-103B is used for the Rafale aircraft weapon and navigation system.
- GAM-T-103C, available in French and English, is interfaced with a LLC1 data link service to support the Recital bus (deterministic Ethernet). GAM-T-103C is used for the new French aircraft carrier weapon and navigation system.

Public Message System. ATLAS 400 is a public messaging system based on ITU-TS MHS X.400-1984 and is a good illustration of the national implementation of X.400 standards. Administration and design of ATLAS 400 is under the responsibility of TRANSPAC, a public company that is a subsidiary of FRANCE TELECOM. The ATLAS 400 services can be provided to private companies or administrations, and different kinds of systems can be built:

- A large company can get its own "private" messaging system, and all the nodes can be split throughout the country at the different company's locations.
- It is also possible to get a system that allows different organizations (public or private) to exchange messages between them. This can be useful, for example, to exchange documents between provider and client. Such an implementation would be used to exchange information between different companies.

ATLAS 400 is only an interpersonal messaging system, and so uses only the Interpersonal Messaging Protocol from the X.400 Series. ATLAS 400 can also be adapted to the size of the

company's computer equipment. For example, the Message Transfer Agent may be locally implemented or derived from the ATLAS 400 implementation. Thus, the User Agent and the Message Transfer Agent are not necessarily co-resident. This illustrates the possibilities of tailoring the system to client use.

SICF. SICF is the French Army battlefield CCIS designed to provide ADP facilities at headquarters at Division, Corps, and levels at field Army and above The elements of SICF are the following :

- Functional Units
  - Each command post has several computers connected to a LAN.
  - Each computer can serve:
    - 12 alphanumeric terminals in any chosen role, such as maneuver, intelligence, or logistics
    - 4 high-resolution graphic cells for maneuver and intelligence
    - 4-auto-dial devices linking into the RITA communications network.
  - Each screen can play any role for the user (G2, G3, etc.).
  - The first-generation uses civil hardware protected by reinforced boxes.
  - Application software has been developed in C language and uses the UNIX operating system.
- Time scale
  - First generation
    - 1988 Stage—Army, Corps and Rapid Deployment Force HQ
    - 1990 Stage 2—Down to division level
    - 1991 Stage 3—Additional functions such as command post flip flop, ISO communication software on the bases of the Quadrilateral Technical Interface Design Plan
    - 1994—Additional logistics functions
  - Second generation
    - 1996—Integration of environment constraints, decision supports, and ruggedization.
- Functions
  - Communications: Computers can be connected to those at other command posts to exchange data, including graphics, via RITA.
  - User Assistance: Computer-assisted message preparation for LANDREP and STANAG 5621/5624 messages; message transmission via RITA and distribution within command posts; automatic production of graphics and situation reports from stored data.
  - Database Management: Distributed relational database.
  - Specific functions: nuclear, biological, and chemical; engineer; intelligence; maneuver; logistics; fire support; and air-space management.

Tactical Profiles. A mixed profile has been defined for use in three interoperable systems in France: the SIR (Systeme d'Information Regimentaire) ABC, the LECLERC tank, and the Tactical Terminal System (TTGC), each being developed by different companies with different physical architectures. SIR is a set of coherent subsystems adapted to a wide range of users and platforms (armor, infantry, engineers, and light forces) designed to provide advanced voice and data communications capability to the regimental units on the battlefield. SIR's Transmission Subsystem provides data transmission between data terminals with messaging applications as well as voice communications. SIR ABC is the SIR subsystem for armor. Its data terminals are workstations located in the command post vehicles at regiment and squadron level, connected by Ethernet (ISO 8802-3) within each vehicle. Communications between vehicles are provided by

VHF combat net radio based on the PR4G receiver. SIR ABC must interoperate with the messaging system of the LECLERC tanks and with tactical data terminals of the support vehicles. The elements of SIR ABC are [Ref. Di Pasquale 1993]:

- Radio and its transmission procedures
- Server that handles the interface between the data application and the radio
- Data application that processes the information and delivers the messages to the server for transmission.

Two transport profiles have been selected for SIR, each containing a new transport standard (ISO+) to support point-to-multipoint transmission: (1) mixed profile, adapted to a mixed voice and data transmission protocol of the PR4G; and (2) TD profile, adapted to a data-only transmission protocol (PAS) of the PR4G. The services and protocols for these profiles are described as follows [Ref. Di Pasquale 1993]:

- ISO+ is a connectionless-mode service offering point-to-point and point-to-multipoint transfer of data of limited size with selected acknowledgments, meaning that the source entity may specify which destinations are required to acknowledge. No reordering of transport service data units is provided. In order to adapt to the potentially different underlying network layers, the ISO+ transport layer performs TSDU segmentation and reassembly. ISO+ is derived from ISO 8602.
- The network layer has minimum functionalities, containing a null version of ISO 8473 (the full ISO 8473 layer could be provided if and when necessary).
- The lower layer of the TD profile, called PAS, is a PR4G procedure that provides transmissions of a maximum of 512 bytes to one or more users. The service offered is a point-to-multipoint or broadcast datagram. It is accessed through the Access to the PAS Service (APASS), which defines how the PAS procedure is used in the profile.
- The lower layer of the mixed profile is call Operational Messaging (OPM). It provides the transmission of a limited number of bytes (1,000 bytes maximum) using the OPM-message-transmission and TDMA procedures of the PR4G. The service offered is a broadcast datagram. It is accessed through the Access to the OPM Service (AOPMS), which defines how the OPM and TDMA procedures are used in the profile.

RA90.[130] The RA90 communication network is aimed at carrying the operational and general-purpose traffic of the French Air Force. It forms the ground-ground segment of the SCCOA (Systeme de Controle et de Commandement des Operations Aeriennes), the French part of the NATO Air Command and Control System (ACCS) that interconnects entities such as air base local area networks and PABXs. RA90 is foreseen to be the backbone of the future French joint transit network to be used by Army, Navy, Air Force, and governmental authorities and is expected to be realized under the control of DGA-STEI (Service Technique de l'Electronique et de l'Informatique). This realization took the benefits of the already operational RAMSES and TELEMAC networks that have validated architecture and operational concepts based on a multiservice capacity using ATM.

RA90 includes a transit network interconnecting LANs and MANs of the Gendarmes, Joint Staff, Air Force, Army, and Navy. The basic platform (Thompac2G) provides such services as X.25, LAPD, binary integrity, SMDS connectionless server, ATM interfaces, end-to-end transparent data links, and video conference (isochronous interfaces).

130 This section is based on excerpts from [Moraisin 1993].

French military initiatives in open systems environments (OSEs).[131] The first attempt to use OSE concepts in military programs began a few years ago during the development o the French CCIS SICF by an intuitive approach. At the present time, the French work in this domain consists in the formalization of these concepts through experimental projects. The aim of these initiatives is to favor the software reusability and portability, to improve interoperability between basic services of systems, and to decrease the development and evolution costs.

Those projects are elaborated around the concept of integration infrastructure *(Structure d'Accueil)*, reusable in any CCIS realization (see Figure 33). It is a Generic Kernel that provides a set of programming interfaces and enables an easy integration of specific operational applications in CCISs. The two main experimental projects are briefly described in the following paragraphs.

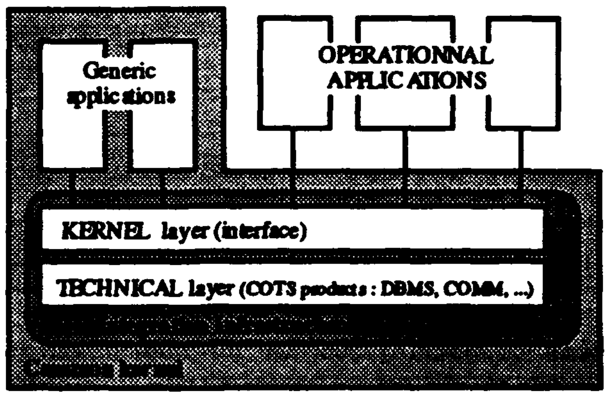


Figure 33. Integration Infrastructure Concept

BDSIC Project. The aim of this project is to demonstrate the operational interest of such a structure within the context of CCIS developments. The prototype realization is based on the following research areas:

- Development of structured data management services that are independent of operational applications (e.g., thematic research)
- Internal interoperability between distinct functional entities
- External interoperability with heterogeneous databases
- Security management
- Enhancement of database management system services (e.g., data dictionary).

The elaboration of a Generalized Data Dictionary satisfies an operational need for data model harmonization within the CCIS.

ISOTROPE Project. ISOTROPE is a leading project that is managed in coordination with several studies, particularly with the BDSIC project. Its purpose is to harmonize and standardize the concept of Integration Infrastructure. This approach is based, on the one hand, upon the existence of COTS products that implement standards offering good guarantees of evolution; and, on the other hand, upon the provision of common services among CCIS applications. In this architecture, two software layers have been defined (see Figure 33 above):

---

131 The remaining paragraphs of this section are based on an informal communication from the French delegation to the January-February 1994 ATCCIS PWG.

one is oriented on common technical services and the other is oriented on operational applications. These two parts of the architecture may be described as follows:

- Integration Infrastructure. As illustrated in Figure 33 (above), the Integration Infrastructure offers a set of standardized services in data management, communication, security, and system management. It is composed of the following:
  - A COTS product sublayer, which enables a CCIS project to limit the development costs and to ensure the evolution of systems
  - A kernel sublayer, based on the one above, which offers a standardized interface for operational applications. This interface enables the independent evolution of applications and COTS products and favors applications interoperability.
- Application Level. The application level is above the Integration Infrastructure and comprises two different types of applications:
  - Generic applications, which are the common basis of CCISs (e.g., MHS, documentation management)
  - Specific applications, which are adapted to particular operational needs and which are based on the Integration Infrastructure services and on the generic applications when needed.

19.4 Germany

HEROS-2/1 is the German Army CCIS that supports staff work at the corps, division, brigade, and battalion echelons.

HEROS Functional Units. The core of this system comprises the computer/communications cabins (RKK) and the graphics cabins (GIK), which are installed in shelters, thus making them fully mobile. The command post can be configured for specific echelons. They are interconnected via a Local Area Network (LAN) allowing command post workstations (GAP) with multi-terminal computers to be linked at remote locations.

For use at the battalion level, the functionality of the RKK and the GAP is combined in a communication-capable command post workstation (GAP-C), thereby providing leanness. The GAP uses a UNIX-based processing unit with a Risc 3000 processor; three MS-DOS user terminals (X-Terminal 425 with Intel 486 at 25 MHz); and a printer, with fiber-optic cable connection and modem to support an ISO 8802-3 local area network. The GAP-C will augment the GAP equipment with communication interfaces to interface to the existing Wide Area Network (WAN) and VHF-radio. The RKK has a UNIX-based Risc 5000 processor, two terminals for system administration, and additional communications (e.g., modems and encryption devices to support 1,000 m of fiber optic cables interconnecting GAP and GAP-C facilities). Most of the hardware and software components used are COTS products.

Each command post can be duplicated in order to provide to the commander high availability of the system and to support the leap-frogging concept. Each workstation can play any role for the user (G2, G3, etc.). Communications to the command posts are provided by wide area networks.

HEROS Functions. All GAPs are capable of handling and displaying graphical military situations/operational plans in front of digital military maps (overlay technique). Formatted messages can be displayed automatically in a graphic form using NATO Standard Tactical Symbols. Vice versa, tactical symbols/situations or operational plans generated graphically by the user can be transformed automatically into formatted messages/texts. The structure of individual "standard situations" can be defined by the user, the content of which will be extracted automatically from the actual central command post database. The staffs of corps, division, and

brigade echelons are also equipped with graphic shelters (GKs). The GK contains a workstation and digitizing equipment with which operational plans can be drawn on a military paper map in large format and fed into the system for further processing. An A0-plotter within the GK allows for the plotting of any graphical situation displayed.

HEROS Applications. The HEROS applications include handling of the following:

- Message formats according to STANAG 5500
- Message reporting based on STANAG 5621
- Orders according to STANAG 2014
- Tables
- Graphical situations/operational plans
- Military Message Handling System
- MMI (X-Windows, OSF/Motif).

HEROS also includes a communications architecture that allows the automatic use of the following communication links:

- LAN (command post communication)
- WAN interconnections
  - Bundeswehrgrundnetz (connection to the Army Staff and NATO)
  - AutoKo (connection to corps, division, and brigade)
  - VHF Radio (connection to battalions and other command posts)
  - QIP-Interface (connection to MCS, SICF, and WAVELL)
  - SATCOM (INMARSAT, INTELSAT) for out-of-area deployment.

HEROS Database Management. Besides other data areas, each command post has available a central, actual, and consistent database that is continually updated by the users according to the occurring events. For redundancy and leap-frogging purposes, this database can be duplicated within a command post. In this case, both databases are held on the same information level automatically.

HEROS Time Scales. Field trials during 3Q 1989 to 4Q 1990. Procurement/fielding in three lots (due to fund limitations). First lot under contract for fielding of the bulk of Crisis Reaction Forces including multinational staffs [e.g., EUROCORPS, GE/NL corps, MND(C)] during 1994 to 1997. The remainder of Crisis Reaction Forces and the Main Defence Forces are planned to be fielded by the second and third lot during 1998 to 2000.

ISDN Implementation.[132] The German Armed Forces decided in 1989 to implement an ISDN network exclusively for their own use. Work is underway to integrate ISDN switches for this network, called the ISDN for the German Armed Forces (ISDN-BW). This network will provide digital connections between all digital end users, different services at one service point with a universal interface, and integration of new services. A migration concept is based on the strategy to replace, step by step, the analog switches in the network by digital switching technology. These digital islands will then be connected with digital transmission links to the ISDN-BW.

Alcatel has proposed an implementation for ISDN-BW based on commercial off-the-shelf products used in the German PTT. Elements of this implementation include: Special Network Exchange (SNE), supporting up to 19,000 analog and 8,500 digital subscribers; Special Network

132 This section is based on excerpts from [Strobel 1993].

Exchange-Small (SNES); Special Network Concentrator (SNC); Special Network Operation; and Maintenance Center (SNO), and PCM30 multiplexer. The multiplexer will have special signalling converters (KZUs) for conversion from analog to digital signalling procedures.

Messaging. A small team at Forschungsinstitut für Funk und Mathematik (FFM) implemented a Message Store (MS) conformant to the CCITT Recommendation X.400/1988, including an X-Window-Based Remote User Agent (XRUA) and a flexible interface of the access to the MS services. Applying an MS, the User Agent (UA) of a Military Message Handling System (MMHS) can run on a small computer because there is no Message Transfer Agent (MTA) needed. The MS releases the User Agent (UA) from the need of 24-hour availability. The system presented will be used for the implementation of military enhancements and it is part of the German contribution to the NATO project CNSI (Communication Systems Network Interoperability) of Subgroup 9. [Ref. Haak 1993]

19.5 The Netherlands[133]

ZODIAC. The Zone Digital Automatic Cryptographic (ZODIAC) network is the tactical communications network of the Royal Netherlands Army (RNLA), whose standards are based on EUROCOM D/1 basic parameters [Ref. EUROCOM D/1 1986]. ZODIAC is a circuit-switched trunk-node network (TNN) used primarily as a voice network but it has the capability for data communications. The nodes are connected via line-of-sight connections. Networks identified as potentially suitable for connection to ZODIAC are the following [Langeveld 1993]:

- Analog PTT networks [public switched telephone network (PSTN)]
- DataNet1 (NL packet switched data network)
- Group Special Mobile (GSM) network (car telephone network)
- ISDN and Internet
- Netherlands Armed Forces Integrated Network (NAFIN), the NL future strategic network, with possible ISDN access capabilities.

The evolution planned for ZODIAC is the direction of the NATO Tactical Communications Architecture being developed by TSGCE PG6. The requirements of this architecture include the following [ATCA MC277/2 1990]:

- Connection of a tactical trunk node to a NATO or national fixed or strategic network, using multiple STANAG 5040 (analog) interfaces or, if both the networks are digital, the use of the NATO Multi-Channel Digital Gateway (STANAGs 4206-4213). This connection must allow transit as well as access connections through the network.
- Connection of a tactical trunk node to a (national PTT) PSTN.

The NATO requirements document [ATCA MC277/2 1990] describes only the NATO interconnection needs (both access and transit) of tactical networks. It does not specify the protocols or mechanisms needed at the strategic or post-telephone-telegraph (PTT) side to realize the interconnections. [Ref. Langeveld 1993]

The ZODIAC network has several interfaces available for interconnection with other (tactical) networks. These include a EUROCOM gateway for interface to the EUROCOM network; an international access link (IAL) for interface to EUROCOM equipment; STANAG 5050 and STANAG 4206-4213 gateways for interfaces to non-EUROCOM networks; and an L1 interface

133 This section is primarily based on [Prast 1994].

(currently a modification of STANAG 5050, as this interface is not yet defined by EUROCOM) to the PTT network. [Ref. Langeveld 1993]

The RNLA is investigating a ZODIAC-ISDN gateway interface based, in part, on STANAGs 4206-4213. ISDN is not yet fully operational in the NL PTT, but there is a pilot project interconnecting several Dutch cities. The gateway is focused on the time-division multiplexing (TDM) primary rate access (European) standard of 2.048 Mbps (30B+D), the 64-kbps, 8-bit pulse-mode modulation A-Law (European) and u-LAW (US) standard speech coding, LAPD, I.441 (Q.921), and I.451 (Q.931). The scope of the required gateway conversions is indicated by Table 71. EUROCOM uses multiple sampling and majority voting (MSMV) and block-code forward error correction (FEC) for data communications. For its subscriber numbering plan, ZODIAC uses STANAG 5046 (*The NATO Military Communication Directory System*), STANAG 4211 (*System Control Standards*), and STANAG 4214 (*Directory for Tactical Communication Systems*), whereas the ITU-TS numbering plan is based on E.163 (Q.11), *Numbering Plan for the International Telephone Services*, E.164 (I.331), *Numbering Plan for the ISDN Era*, and I.330, *Numbering Addressing and Routing*. A study by RNLA has concluded that a ZODIAC-ISDN based on STANAGs 4206-4213 is feasible and may be used to interconnect other networks, such tactical-to-FDDI networks. However, since the STANAG 4206-series interface was originally developed for a tactical gateway, some changes (e.g., the possibility to exchange signalling information before traffic mode is reached) in the existing STANAGs may be necessary to make the interface useful. [Ref. Langeveld 1993]

Table 71. Overview of ZODIAC-ISDN Gateway Conversions

Conversion Type	ZODIAC (EUROCOM-based)	ISDN (PSTN/Strategic)
Trunk Speed	256 kbps	2048 kbps
Speech Coding	Delta Modulation	PCM (A-Law)
Numbering Plan	STANAG 4214	I.330
Protocol	STANAGs 4207, 4208	Q.921
Data Communication	MSMV/FEC	Asynchronous/Synchronous
Security	ZODIAC	PTT/Strategic
Management	ZODIAC	PTT/Strategic

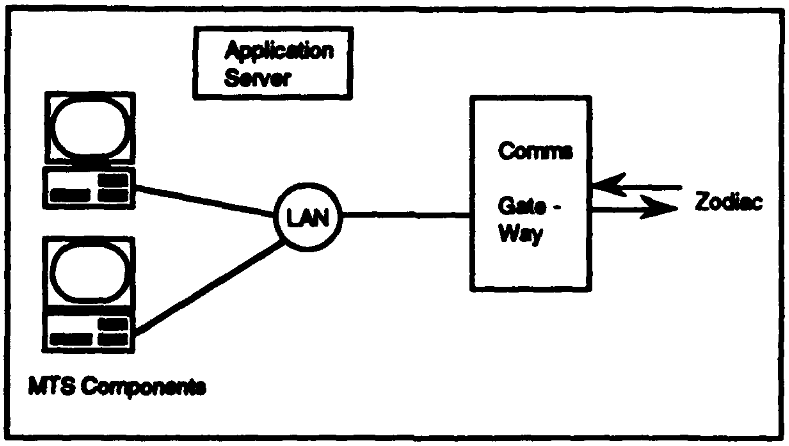
Source: [Langeveld 1993].

Message Transfer System (MTS). In December 1994, the new MTS will be fielded, upgrading the present store-and-forward system for teletype messages. The MTS will make full use of the ZODIAC infrastructure, with the added benefit of error-free data transmission. Although primarily intended to handle the voluminous ACP-127 teletype traffic, it will also comfortably handle file transfer. The relation of MTS to ZODIAC is illustrated in Figure 34. To guarantee delivery of all messages accepted for transmission, the messages are replicated to a maximum of three other message switches using the ZODIAC network.

The following comments on standards apply to the MTS:

- Standard X.400 does not meet the military requirements for priority and security levels, compatibility with ACP 127 and military addressing. A set of protocols, based on X-400 and designed to be used over the EUROCOM-compliant ZODIAC network, was developed.
- LKBP is an application layer Message Handling protocol, based on STANAG 4406 (military extensions of X.400). Gateways will handle communication with non-LKBP systems, including conversion of ACP-127 messages.

- LKDP is a protocols stack covering OSI Layers 1 through 6 in the ZODIAC environment.
- COTS products covering formal and de facto standards are used where possible. HDLC, for instance, is used to ensure error-free transmission of text and data.
- The MTS has been designed to effect a transition to X.400, if and when necessary, with minimal effort.

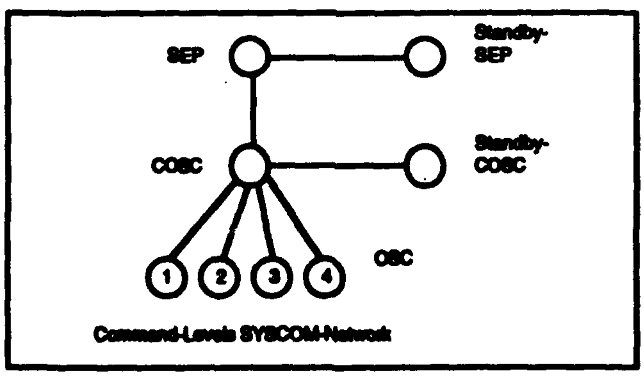


Source: [Praat 1994].

Figure 34. MTS Employment in Zodiac

System Control and Management (SYSCOM). SYSCOM supports the management of the RNLA ZODIAC communications system. The management of ZODIAC has been divided into the three hierarchical levels identified by EUROCOM, with an extra coordinating layer for Signals Regiment Operations. The main functions of the SYSCOM-network have been allocated to the following roles (see Figure 35):

- System Execution and Planning (SEP)—supporting for operational planning: overall management of frequencies:
- Coordinating Operational System Control (COSC)—allocating resources
- Operational System Control (OSC)—managing operational units and equipment, performing frequency calculations, and managing communications links
- Facilities Control (FC).



Source: [Praat 1994].

Figure 35. System Control and Management in Zodiac

All SYSCOM hardware and software configurations are identical. A system can thus support any role at any level. A subset of the functionality is made available to the user, depending on the role and the hierarchical level of the unit at that time. Because changes in data replicated to all other cells, every cell can take over any SYSCOM role at any level at all times.

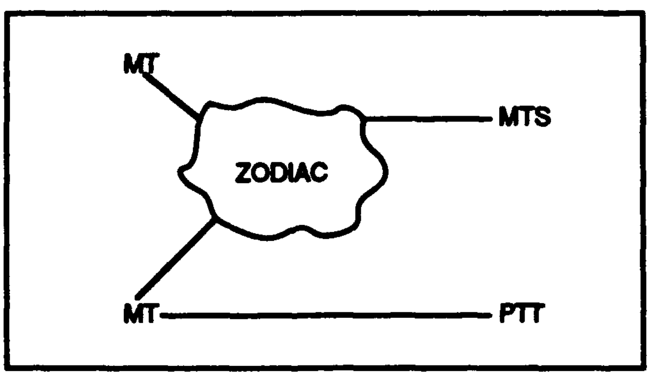
The following comments on standards apply:

- Because the SYSCOM system uses the ZODIAC network, communications must meet the requirements of the EUROCOM standards D0 and D1.
- The original plan was to link the SYSCOM cells using X.25 for Layers 1-3. Because of problems with the COTS software, TCP/IP over DECNET is used in the operational system.

Message Terminal (MT). The MT will be fielded in September 1994, replacing the current Personal Computer Teletype (PCT). It combines the functionality of the X.400 User Agent (to edit, send, receive, store, and manage messages) with that of a standard (portable) office personal computer. It can also function as an Access Unit for teletype messages.

Since the MT will be deployed in national and multinational (NATO and UN) operations, the MT user interface has been written in English. For the same reason, the MT supports both ACP-127 and LKBP/LKDP. It is also possible to edit a free-format header to suit other standards.

In the ZODIAC environment, the MT is connected to the data port of the secure telephone. Messages and data can be sent point-to-point or via the MTS store-and-forward system. In other environments, point-to-point links can be established via PTT or SATCOM, using modems. Equipment for on-line encryption can be added if required. The role of the MT in ZODIAC is illustrated in Figure 36.



Source: [Prast 1994].

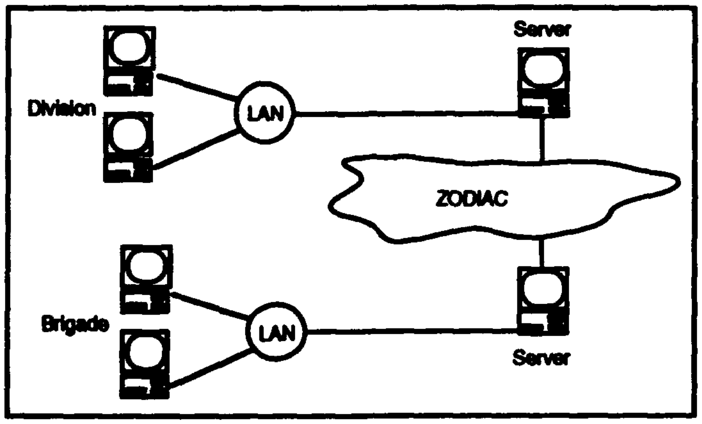
Figure 36. Role of Message Terminal (MT) in Zodiac

The following comments on standards apply:

- The MT uses the X.400-based LKBP and the EUROCOM-compliant LKDP in the ZODIAC environment.
- Elsewhere, the MT supports ACP-127 over ITU-TS V.24/V.28 links.
- MS-Windows provides the required multi-tasking capabilities on an Intel platform, as well as the graphical user interface.

CCIS Program Evolution: Software. The RNLA has substantial in-house software development resources. Its in-house capability has been involved in C2-related projects for a number of years, in the roles of technical authority, sub-contractor, or main contractor.

One of the key projects is the development of a prototype CCIS for brigade-level to corps-level headquarters (see Figure 37). Initially, its main function is to create a common "information base", both within a headquarters and across unit boundaries, that is readily accessible. Read and write access is through a Windows-Icons-Menus-Pointer (WIMP) user interface over a map background. Information on a unit's location, status, plans, and holdings is represented in standard military symbology, with additional alphanumeric data only a mouse click away. Color codes, warning messages, and a high proportion of user-selectable view options help to fulfill an individual user's information requirements. High-quality overhead projection supports briefing and presentations. Within an HQ, the workstations in cells are connected via an Ethernet LAN. Using point-to-point data links over the ZODIAC network, data is replicated to other HQs.



Source: [Prast 1994].

Figure 37. Support of Division and Brigade Echelons in ZODIAC

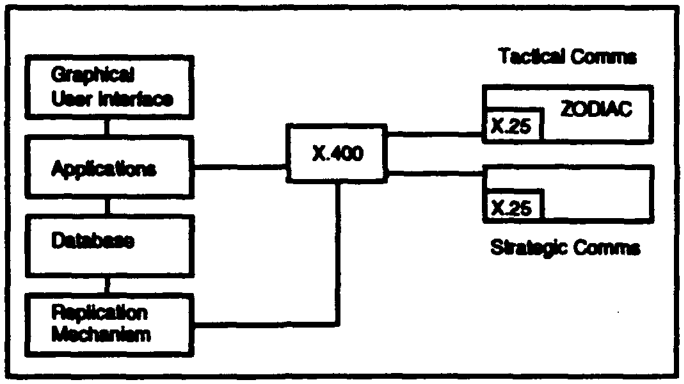
Experiences with several iterations of the prototype on maneuvers have shown the concept to be viable. The intention is to validate it formally, convert it to the ATCCIS architecture, and then to field an implementation of the core capability. The hardware and software architectures have sufficient flexibility to be able to add functionality when necessary. The present prototype will be the point of departure for the development of the RNLA contribution to the ATCCIS Phase III demonstrator in 1995. For the prototype, de facto standards supported by COTS products on the current hardware platform (Sun workstations) have been used: TCP/IP over Ethernet, GKS, Open Look, and SQL. The ATCCIS architecture and the OSE model are expected to influence the final implementation considerably.

CCIS Program Evolution: Platform. Fully functional CCISs perform a common set of tasks for all users and provide additional functionality depending on role and mission. The current political situation has led the Dutch Government to task the RNLA with a variety of roles and missions that call for a flexible Army and, consequently, also requires great flexibility in its CCIS.

A fully functional CCIS also needs a substantial amount of computing power for a variety of tasks: transactions on sizable databases, graphical user interface, raster and vector geographical data, processing for complex algorithms, and local and wide area network connections.

To be able to meet these requirements, the RNLA has developed the concept of a highly modular Universal C2 Workstation (see Figure 38). Based on the OSE and the ATCCIS

architecture, these workstations and the CCIS they are part of will provide a common core database, applications, and communications facilities. Additional capabilities can be added for specific mission or needs of a subfunctional area on a temporary or permanent basis.



Source: [Prast 1994].

Figure 38. Architecture for Universal C2 Workstation

Geographical information plays a crucial part in a CCIS. The system must be able to function with a minimum of raster data, providing more functionality when more data becomes available. DIGEST is at present the preferred format for acquisition of digital terrain data, while others are under consideration.

COTS products, based on international standards, will be used for implementation of the concept. Fielding is expected in 1996. The RNLA is committed to use the work of civil and NATO standards organizations where possible.

19.6 The Netherlands, Norway, France, United Kingdom

Four NATO nations are participating in a project entitled "Cooperative Prefeasibility Studies for Tactical Communications Systems for the Land Combat Zone—Post 2000." In this study, candidate subsystem architectures are being developed on the basis of current and near future communications technologies as ISDN, EUROCOM, FDDI, PABX, packet radio and cellular telephony. From these technologies six subsystem architecture alternatives were derived each with either a nodal (centralized) or a nodeless (distributed) characteristic.

From this set, subsystem architectures are selected on the basis of military operational requirements and threat expectations to form one system architecture for the entire Land Combat Zone. The chosen system architecture to cover the intermediate and the rear zone of the land combat zone. The wide area communications subsystem consists of a backbone of distributed Local Area Communications Subsystem (LACS) elements with centralized LACS elements providing access to the backbone. [Ref. van der Voort 1990]

19.7 Norway

TADKOM.[134] TADKOM is the Norwegian tactical area communications system. The packet radio segment for TADKOM will be the multi-role radio (MRR). The Norwegian Defence Digital Network (NDDN) is the Norwegian strategic network. Compatible services for NDDN for

134 This section is based on excerpts from [Knutsen 1993].

the tactical area are under study. X.400 (1988) and ACP-127 message handling are already in operation for NDDN. This capability has been updated to conform with MMHS-88 (STANAG 4406). In the future, tactical message switches (TMSs) will be installed in command posts, where there will be operator positions for management of the tactical MHS as well as for traffic handling. The TMS will contain functions to support message handling services for packet radio subscribers. X.25 and circuit-switched connections are planned. There will be an extension of S.25 for connectionless data units in TADKOM.

The radio units in the MRR will be called tactical multirole radios (TRRs). The TRR will be used in two applications: tactical radio access system (TRAS) and combat net radio (CNR). The TRR provides access to voice (16-kbps CVSD) and data services (packet data using S.25 with extensions for connectionless transmission). Protocols for Layers 1-3 for CNR and TRAS will be only slightly different and offer the same services to the higher layers.

The use of MMHS and protocols identified above is expected to meet interoperability requirements and support efficient use of radio bandwidth. The proposed protocols support both radio silence and periodic unavailability by means of a message store and letting the radio choose when and what to send and receive. For short messages, which are very important in a tactical environment, the reduction in overhead compared to full X.400 is expected to be at least 10:1. This is mainly the result of transmitting only required information associated with the X.400 protocols, leaving out Layers 4-6 to reduce both the number of bits sent and the delay.

19.8 Spain

Spain. The SP MOD is using and is projecting to use more and more components based on OSI standards. Support of the SP Defence C3 System currently consists of the following:

- Hardware:
  - Workstation Digital (MICROVAX)
  - Servers (Tektronics)
  - PC-compatible workstations
- Software:
  - Digital/VMS
  - Tektronics/UNIX (System V)
  - PC Compatible/SCO Open
  - X-Windows, Motif, MS-Windows 3.1
  - ADABAS database management system
  - ACP-127 formatted messages.
- Internal communications:
  - Ethernet (ISO 8802-3)
  - TCP/IP and DECNET protocols
- Communications system standards:
  - FAX/telephone—PTT (PSTN) and PSN
  - Data net interface—X-25
  - Protocol—LAP-B
  - Connection of PSTN-DSN—X-28 and X-32
  - Messaging—ACP-127
  - Messaging upgrade—X-400 with ACP-127 gateway and MHS (X.400:1988).

19.9 United Kingdom

Robust Protocols Research Programme. The UK MOD and NATO has established the Robust Protocols Research Programme at Defence Research Agency to quantify and minimize the risks associated with the UK MOD and NATO policies for procuring future CCISs to ISO OSI standards. The approach being taken is to take commercial off-the-shelf protocols that are as near as possible to the perceived military requirement. The performance of these protocols is being established under ideal and degraded conditions in the laboratory.

Initial work has concentrated on the X.400 and FTAM standards. A protocol stack, using X.400 or FTAM, Transport Service Class 4 (TP4), and connectionless network service (CLNS) over X.25(1984) has been selected. These were selected to give a worst case scenario for evaluating the protocol standards. Early results have provided an upper bound to the overheads that may be experienced under ideal conditions. This result will be used for the design and sizing of messaging networks. Some measurements on the performance of FTAM over degraded links have also been obtained. These have shown how a more "intelligent" implementation of the data link protocol could provide optimum throughput over a range of degraded conditions. [Ref. Price 1990]

Defence Fixed Telecommunications System (DFTS). MOD Central Defence staffs are establishing a Defence Packet Switched Network (DPSN). This project is a major element of a broader Defence-wide communications infrastructure covering all communications services: the DFTS. Over time, the present MOD and Armed Forces communications systems will integrate to DFTS. Profiles that have been recommended for the DFTS are of three types: end-system services, common application services, and basic communications services. End-system services, together with the proposed standards, are electronic trading (based on EDI), revisable document exchange (based on ODA), general file transfer (based on FTAM), remote terminal access (based on VT), inter-personal messaging (based on MMHS), and inter-organizational messaging (also based on MMHS). Common application services include message handling (MMHS), Directory, ACP 127 interworking (MMHS), shared file store (FTAM), and shared database (RDA and SQL). The basic communications service profiles are T.31(M) for WAN access, T/611 and T/613 for LAN access, R.131(M) for WAN-to-WAN relay, and R/21 for LAN-to-LAN relay. [Ref. Bailey 1990]

The UK MOD has a commitment to provide its single-Service strategic communications needs via a common communication network (DFTS). It is also MOD policy that such provision should, to the greatest extent possible, be procured from the civil market to standards recognized by the international community. Progress in implementing the DFTS has been slow as the priority of each of the Single Services has been to deploy their own systems, leaving convergence to DFTS until a later date. However, one subset of DFTS, the packet switched data communications network (DPSN), was identified as requiring common provision to satisfy immediate operational needs.

The DPSN procurement has been guided by the DFTS Architecture and Procurement Working Group (DAPWG), which recommended that (1) the network be based upon the internationally recognized X.25 standard for network access; and (2) potential candidate network systems should be mature, have considerable expansion capability, and be supported by a manufacturer with a total commitment to the product and development of the relevant standards. The procurement has been distinguished by the short time scale between statement of requirement

and in-service operation, and being both within the financial provision and satisfying the operational requirement. For the future some significant issues have to be developed and resolved, not the least being interworking with other systems, e.g., ISDN, multilevel security and management across the boundary between DPSN and end-user systems. [Ref. Dibble 1990]

WAVELL. WAVELL is a battlefield ADP system, built to full military specifications including TEMPEST and NBC. It is designed primarily to assist G2/G3 staff cells in headquarters at corps, division, and brigade levels. It has limited G1/G4 functionality. Full deployment to 1 (Br) Corps was completed in 1987 and the latest software upgrade (Version 5) will be tested at the end of 1991, after which no more changes to the existing WAVELL will be made. [Ref. TSGCE 1991n]

Quadrilateral Interoperability Field System (QIFS). In order to provide the ACE Rapid Reaction Corps (ARRC) with international interoperability mechanisms, the United Kingdom, as framework nation, has developed and produced the QIFS. QIFS is the UK contribution to the QIP, which also involves the national army tactical CCISs of France (SICF), Germany (HEROS), Italy (STACCON), and the United States (MCS). Interoperability is achieved by exchanging ADatP-3 messages through X.400 message handling systems. The standards used in QIFS can be effectively divided into two areas: those agreed by the QIP community and those chosen for use on the national side. The standards are as follows:

- QIP standards—modified variant of X.400:1984; X.25:1984, and ADatP-3 message defined in STANAGs 5621 and 5624.
- QIFS national standards—two commercial X.400:1988 products conforming to UK GOSIP 4.0; PTARMIGAN X.25:1980; and the IRIS/Message Formatting System (MFS) application package, which defines and validates ADatP-3 messages. IRIS/MFS is also used in the AMH project within ADSIA. The INGRES 6.4 relational database management system is used to archive all messages, and a network management package has been developed using the INGRES Windows/4GL. All workstations use the Motif/X-Windows graphical user interface and run under either SCO UNIX or HP-UX.

Interim ACE Rapid Reaction Corps Information System (IARRCIS). Project IARRCIS is a system for the ARRC Headquarters and will concentrate on providing the staff officer with the ability to create files in a variety of COTS packages and pass these files over a reliable network to other users. The standards used will be the same as for the QIFS. There may be two operating systems within IARRCIS: where possible a C2 E2 accredited UNIX operating system will be used; where this is not possible, MS DOS may be used.

WAVELL Risk Reduction Exercise (WRRE). The WRRE was an attempt to demonstrate that it would be possible, at low risk, to build a military C2 system from COTS products. The project was commissioned by MOD(UK) and carried out by the Defence Research Agency (Fort Halstead). It used an architecture that included an X.400:1988 message handling systems and X.25 packet-switched network. Some useful lessons concerning procurement of systems built from COTS were learned, but it should be noted that the system built was not a prototype or necessarily an architecture that will be adopted.

UK Army CIS Standards Programme.[135] The UK Army has initiated a program of standardization for its future command, control, communications, and information systems (CIS)

---

135 This section is based on excerpts from [Fowler 1993] and [Sutherland 1993].

aimed at achieving and integrating CIS by 2010. CIS covered by the program will include all systems used on and off the battlefield to support the preparation, deployment, and operations of land forces. An initial stage in the standards program, defining the intercept strategy for common standards approach to CIS procurement, was conducted during May 1991 to January 1992. Remaining stages are to identify and specify common CIS standards; and to identify and specify "environment-specific" standards for operational and support/planning systems that lie outside common standardization areas. This program is an outgrowth of several information system strategy studies begun in 1988 (command, logistics, and personnel), which were combined to form a coherent, consistent Army strategy and Goal Architecture.

Three CIS infrastructures were designated to host the CIS projects: CASH/WAVELL, serving Army Headquarters at and above the one-star level (CASH will service fixed, peace-time headquarters and provide maximum compatibility with Enhanced WAVELL for battlefield use); UNICOM, serving Army units below the one-star level in barracks; and CHOTS, serving MOD Headquarters. MOD has recently decided that CASH will adopt the CHOTS infrastructure. Some standards for these infrastructures have already been defined, further constraining the choice of standards for the CIS program.

At a minimum, the requirement for interconnections is to exchange data, leading to a demand for common communication standards; common data definitions, formatting, and encoding; common formatting of documents and messages; and compatible security arrangements, both procedural and electronic. In the communications area, an internetworking service is needed across all networks, both fixed and tactical. Requirements for the "military network service" include the following, based on UK and NATO studies:

- Security features (peer entity authentication, access control, connection confidentiality, connection integrity without recovery, traffic flow confidentiality)
- Multihoming, mobile hosts, and multi-addressing (broadcast mode)
- Automatic provision for precedence (four levels) and preemption
- Queueing of input traffic and allocation to available circuits to produce defined transit delays.

The primary areas where standards are needed are data management, security arrangements, data communications, and office automation. The program will seek to minimize the number of different environments to facilitate portability between hardware platforms; to save on personnel recruitment, training, and hiring of specialist staff; and save money. Environment-specific standards may be required for geographic information systems, hardware ruggedization, and tactical communications. Standards deficiencies were noted in the following areas:

- Geographical information systems (GISs)
- Video conferencing
- Digital image transmission
- Voice input to computers
- IKBS/KBS (knowledge-based system) applications
- CALS support for integrated logistic systems and CIRPLS.

Table 72 identifies standards currently identified for the UK Army CIS Program by the Army CIS Agency (ACISA).

UK MOD Technology Demonstrator Programme. The UK MOD initiated in 1993 a security and integrity Technology Demonstrator Programme (TDP), which will attempt to develop security standards with wide commercial application and viability. The program is based on bilateral contracts between the MOD and a number of core product suppliers, who will contribute team members to an Industrial College. The College will develop an initial draft standard for a security architecture and an implementation plan. This cooperative effort between industry, government, and commercial users is hoped to provide breakthroughs in the implementation of information technology security that meets end-user needs. A principle challenge will be to ensure interoperability between product sets of participating suppliers and gain acceptance of standards-making bodies such as POSIX. [Ref. Government Computing 1993]

Following endorsement of the scoping study recommendations in October 1992, work has been initiated to set up the Army Communications and Information System Standards Management Organization (ACISSMO) to manage the Army's continuing requirement for CIS standards. It is expected that ACISSMO will be operational by April 1994. In the interim, work has continued to ensure that the standards recommendations continue to be relevant for the Army's requirements. Further work is being done to clarify the recommendations for human-computer interface and geographic information systems. [Ref. Liddell 1994]

19.10 Australia

Centralized planning by Headquarters Australian Defence Force (HQADF) has resulted in a Defence Communications Corporate Plan (DCCP) [Ref. DCCP 1991], which has embraced a move towards increased adoption of global civil telecommunications standards. This plan includes the following recommendations:

A long-term research program, Defence Organization Integrated Communications (DORIC), is under way to define and demonstrate an integrated communications architecture for the Australian Defence Organization into the 21st Century. DORIC is centered around providing a global backbone for C2I traffic and takes into account the possibilities of transporting large databases, video teleconferencing, imagery, sensor data, and intelligence traffic. DORIC seeks to enable current and future traffic types to share common access, switching, and transmission assets. DORIC will address military attributes such as security, survivability, trustworthiness, priority, and preemption. Among techniques being examined is EVEREST, which enables practical adaptive radio systems by rapidly, passively, and accurately estimating the probability of error over non-Gaussian radio channels in an unbiased manner. Experimental ATM switches have been developed.

Table 72. UK MOD Draft Standards for CIS Systems

Title	Intercept Standard	Total Standard	Applicability	Further Work
Dictionary	ISO 10027	ISO 10027	Army	
ODA/ODIF	ISO 8613	ISO 8613	Army	F SS
Messages	ISO 7982 ISO 9735 STANAG 5500 Series	ISO 7982 ISO 9735 STANAG 5500 Series	Note 1 Note 1 Note 1	F F F
CCR	ISO 9804 ISO 9805	ISO 9804 ISO 9805	Army Army	P P
RDBMS	COTS (Note 2)	Not Defined	Army	F P
Graphics	COTS ISO 9636 ISO 8632	Not Defined ISO 9636 ISO 8632	Army Army Army	
GIS	COTS DF (XII)	Not Defined Not Defined	Army Army	F P F P
Office Automation	COTS Various Stds	Not Defined Not Defined	Army Army	 F P
ODP-TP	ISO 10026	ISO 10026	Army	
ODP-DDB	ISO 9075	Not Defined	Army	F SS
ODP-RDB	ISO 9579 ISO 8649 ISO 8649 ISO 8650 ISO 9072	Not Defined	Army	F SS
Terminals	Note 3	Not Defined	Proj	F
Operating Systems	ISO 9945	ISO 9945	Army	SS
3GL	ISO 7185 ISO 1538 ISO 1539 ISO 1989 ISO 6160 DEFSTAN 0546	ISO 7185 ISO 1538 ISO 1539 ISO 1989 ISO 6160 DEFSTAN 0546	Army Army Army Army Army Army	F F F F F F
4GL	ISO 9075 ISO 8652 ISO DP 8485 COTS	ISO 9075 ISO 8652 ISO DP 8485 Not Defined	Army Army Army Proj	F F F
Graphics Kernels	DIS 9636 ISO 8632 ISO 7942 ISO 9592 ISO 9593	DIS 9636 ISO 8632 ISO 7942 ISO 9592 ISO 9593	Proj Proj Proj Proj Proj	F F F F F
Data Store	ISO Various	ISO Various	Army	F
Peripherals	COTS	Not Defined	Proj	F P S
MMI	BSI/ISO Various (see MMS)	BSI/ISO Various	Army	F
HCI	Note 4	Not Defined	Army	F P SS
WAN	GOSIP-T/X.25 SNA Gateway	GOSIP-T/X.25	Army IBM	F S
LAN	GOSIP-T (Note 5)	GOSIP-T	Proj	
LAN/WAN Inter-Connection	ISO 10030 ISO 9542 COTS	ISO 10030 ISO 9542	Army Army IBM	 F

Table 72. (Cont'd)

Title	Intercept Standard	Total Standard	Applicability	Further Work
WAN	GOSIP-T/X.25 SNA Gateway	GOSIP-T/X.25	Army IBM	F S
LAN	GOSIP-T (Note 5)	GOSIP-T	Proj	
LAN/WAN Inter-Connection	ISO 10030 ISO 9542 COTS	ISO 10030 ISO 9542	Army Army IBM	 F
FTAM	ENV 41204	ISO 8571	Army	
VT	ISO 9040/41 COTS	ISO 9040/41	Army Proj	 F S
MHS	ISO 10021 or STANAG 4406	ISO 10021 STANAG 4406	Army Army	F S F S
JTM	COTS	ISO 8831/3	IBM Army	F F
DTAM	CCITT T.430 COTS	CCITT T.430	Army IBM	F F
Characters	Not Defined	Not Defined	Army	F P
N&A	Not Defined	ISO 9594	Army	F
Network Management	ISO 9596 ISO 9595 DIS 10040 DIS 10164	ISO 9596 ISO 9595 DIS 10040 DIS 10164	Army Army Army Army	F SS F SS F SS F SS
Security	CESG	CESG	Army	F SS

Key for Applicability:

Army: Applicable army-wide
Proj: Applicable to group of projects
IBM: Applicable to the A-Area IBM environment

Key for Work:

F: Requirements for standardization need to be clarified
P: The range of products implementing the standard needs to be investigated
S: The standards need to be investigated further
SS: Emerging standards (including de facto) need to be monitored

Note 1: The first standard refers to financial data exchange; the second to EDIFACT, and the third to operational messaging, probably to be NATO-wide using the established ADatP-3 standards.

Note 2: See Rows on Third Generation Languages (3GL)/4GL; SQL is a recommended Army-wide standard that is known to be supported by the leading relational database management system (RDBMS) products.

Note 3: The battlefield environment may require modifications to the mechanical design of QWERTY keyboards, for example, to permit operation by gloved hands, and there may be a continuing requirement for specialized peripherals such as hand-held data-entry keypads, tracker balls, light pens, etc.

Note 4: ACISA is currently investigating the implications of adopting the CHOTS HCI for Army-wide use.

Note 5: Covers profiles for CSMA-CD and Token Ring (8802-3/5/6) and FDDI.

Source: ACISA [Liddell 1994].

19.11 United States

19.11.1 US Defense Standardization Programs

US DTMP Standards Development.[136] This section summarizes standardization activities being conducted in the US DoD related to data communications for open systems implementation. The coordinating body for these activity is the Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP). The work of each of the working groups of the DTMP may be summarized as follows:

- WG1 on Lower Layers—thin stacks for OSI, multicasting; transport profile, simplex profile, Internet profile, and wireless LAN; work on Enhanced Communication Functions and Facilities (ECFF); work on National Imagery Transmission Format (NITF) addressing full-duplex and half-duplex (but not simplex) capability and large-imagery file transfer; protocols for USSPACECOM and liaison with the Space Communications Protocol Standards Technical Working Group (SCPS-TWG), a joint effort of DoD and NASA; Reliable End-System Transport profile
- WG2 on Upper Layers—MHS profile; restricted MMHS profile; FTAM profile; Internet profiles on file transfer, remote login, and domain name system; SMTP; interoperability testing; gaining national and international acceptance of the P772 Military Message content type in MMHS, such as proposing modifications to IGOSS and US GOSIP, working with ANSI and NIST
- WG3 on Security—security labelling (Common Security Label); Message Security Protocol (MSP), including promulgating MSP to the international level through NIST and whether NSA will release key management information required for common MSP usage at the international level; security frameworks and Generic Upper Layer Security (GULS); Secure Data Network System (SDNS)
- WG4 on Network Management—Network Management for DoD Communications; SNMP; managed objects; DoD Network Management Information Model (MIM)
- WG5 on Architecture—Technical Reference Model (TRM) project; conceptual requirements for DoD; identifying holes in the DTMP standards framework; harmonizing DTMP TRM, DoD TRM, and OSE/IA model; networking section of ITSG-OSE (formerly OSE/IA); wireless LAN project (with WG1)
- WG6 on Registration [dissolved in 1993 in favor of the GOSIP Advisory Group on Registration (GAG-R)]
- WG7 on Testing—MIL-HDBK-1350 on testing with separate volumes on protocol validation plan and conformance and interoperability testing plan (this working group may be dissolved following publication of these two volumes); assisting validation of message handling, MSP, and reliable end-system transport imagery
- Liaison and related activities
  - Federal Internetworking Requirements Panel (FIRP)—appointed by NIST at the direction of the Federal Networking Council (FNC) to study issues and recommend long- and short-term actions in connection with the standardization of communications protocols; addressing comparative strengths and weaknesses of the OSI and Internet protocol suites; ease of use, economic impacts, and commitments to other entities such as NATO; convergence of the two protocol suites; possible use of TCP/IP as a prescribed protocol suite in US GOSIP (Version 3 of US GOSIP is being delayed pending recommendations of the FIRP)

---

136 Based on the following sources: [DTMP 1993a], [DTMP 1993b], [DTMP 1993c], [DTMP 1993d], and [DTMP 1994a].

- OIW: Expansion of OIW to increase focus on open systems environment (OSE); new special interest group on multimedia
- OSI Implementation Strategy document—current version compares TCP/IP to OSI and recommends a dual-stack instead of a split-stack approach; three-phase strategy, of which the second is the current phase: (1) increasing OSI protocol experience and implementation of some Application Layer gateways, (2) activation of additional OSI services, and (3) final implementation, requiring the acquisition of fully tested and certified advanced OSI capabilities
- ITSG-OSE (formerly OSE/IA)—provides consistent open systems IT standards acquisition guidance; examines various IT standards categories; prescribes mandatory standards within each area; and provides interim solutions and emerging options to address areas with standards deficiencies.
- DoD E-Mail Strategy—Version 2 of Message Security Protocol (unclassified and approved for public release); convergence of MSP with X.400
- JTSSG: Telecommunications Systems Standards (TCSS) program, FED-STD-1037B, STANAG responsibility; Federal Wireless Users Forum (FWUF); Tri-Service Open Systems Architecture Working Group; Defense Standardization Program (DSP) Mission Critical Computer Resources (MCCR), which is establishing an opens systems architecture for embedded weapon systems; Imagery Standards Management Committee (IMSC)
- ITU-TS OSI Efficiency Meeting
- Internet Engineering Task Force (IETF)—TCP/IP-OSI migration issue; IP Next Generation Meeting; working groups on IP over Asynchronous Transfer Mode (ATM), TCP/User Datagram Protocol (UDP) with Big Addresses (TUBA), Internet Protocol Security Protocol (IPSEC), and Inter-Domain Multicast Routing (IDMR); potential problems with the Network Layer Security Protocol (NLSP); 11 functional areas in IETF with working groups established to work on separate issues in each area
- Defense Information Infrastructure (DII) and US National Information Infrastructure (NII)
- Support for and review of drafts for next edition of WP 25.

US Space Command (USPACECOM) Standardization. The Space Communications Protocol Standards Technical Working Group (SCPS-TWG), a joint effort of DoD and NASA, is an effort initiated to provide open systems capabilities for the North American Air Defense (NORAD) USPACECOM Integrated Command and Control System (NUICCS), which is the C2 infrastructure that supports the commanders-in-chief (CINCs) of NORAD and USSPACECOM. The NUICCS is composed of over 200 major elements, command centers, communications networks, and data processing systems. New mandatory terrestrial communications protocols have been defined (N/SP-STD-1100B) that are fully US GOSIP compliant. Additional work by the SCPS-TWG is focused on reducing the overhead of OSI protocols to make them more usable in the bandwidth-limited space environment. Other standards work includes the use of application-process-to-application-process message-embedded cyclic redundancy check (N/SP-STD-1500A); standard structure for formatted messages and message sets (N/SP-STD-1700); and real/test/exercise capabilities standard (N/SP-STD-1900). [Ref. DTMP 1993a]

Common Data Link (CDL) Program. DISA/DSPO has initiated the CDL program to ensure interoperability at the data link operations level and to provide commonalty to reduce development and support cost. DSPO has developed an IC3 architecture whose goal is global C3 via selected satellites. Studies are being conducted or planned on architecture, partitioning, commercial standards, waveforms, data formats, protocols, networks, interoperability issues, and

acquisition techniques. Standards anticipated for CDL include moderate-rate LAN interface in 1995, high-rate bus interface in 1996, and high-rate LAN interface in 1998. [Ref. DTMP 1993a]

ITSDN Program and Standards for US DoD.[137] The US DoD has developed, coordinated, and validated a program plan [Ref. DISA 1992] for the Integrated Tactical Strategic Digital Network (ITSDN) to focus DoD's efforts to attain tactical-to-strategic and tactical-to-tactical data communications interoperability. This plan is an outgrowth of a 1989 demonstration of the use of packet switching technology and end-to-end encryption (E3) technology in the military tactical system environment. That demonstration, using BLACKER, showed that tactical data networks could be connected to, and made to interoperate with, the strategic Defense Data Network [DDN, now the Defense Information System Network (DISN)].

The ITSDN program has been charged with identifying solutions for interconnectivity and interoperability between data networks supporting strategic, CINC, JTF, and tactical data systems, providing for the following:

- Tactical access to national and strategic information resources
- Multi-level secure data communications
- Use of standard protocols and interfaces
- Improved bandwidth utilization
- Emphasis on the use of commercial and non-developmental solutions
- Architecture based on compatibility with Service tactical data network plans, with minimal equipment introduced in theater to support ITSDN
- Basis for tactical evolution to US GOSIP.

ITSDN will be based on the use of the DoD standard protocol suite, with an undefined migration to GOSIP protocols. A mixed stack X.400 over TCP/IP is expected. Interconnection and two-way data exchange across system boundaries at multiple security levels will be accomplished according to a jointly defined and validated security architecture (yet to be developed). However, the systems to be interconnected have very different security architectures and include schemes for physical separation of traffic at different security levels, cryptographic separation of traffic at different security levels, system-high security protection, and human-in-the-loop security mechanisms. Available mechanisms include E3, label-based mechanisms, guard devices, and application layer security protocols, which will need to be implemented in an evolutionary fashion as the technology to support the mechanisms matures. The following are examples of networks to be interconnected using ITSDN:

- DISN, which is composed of four separate worldwide packet switched networks: MILNET (carrying unclassified and sensitive traffic); DSNET1 (secret), DSNET2 (top secret), and DSNET3 [top secret/special compartmented information (SCI)]. DISN is evolving to include provision of high-speed data switching and routing using IP routers, providing users with connectivity options such as X.25 networks and high-speed IP networks. Strategic DISN subscriber systems will be migrating to GOSIP protocols, and the DISN will provide network support for GOSIP users.
- Tactical switching systems such as Mobile Subscriber Equipment (MSE), Tactical Secure Data Communications (TASDAC), and Tactical Communications Distribution Node (TCDN).
- Information exchange links in Copernicus.

137 This section is based on excerpts from [Pennington 1993].

Secure Tactical Data Network (STDN) Demonstrations.[138] ITSDN program participants recognized early that the integration of the strategic and tactical communications security architectures would pose particularly difficult problems from both a policy and technological standpoint. The strategic network security architecture was developed as part of the DISN-Near Term (DISN-NT) program largely without regard to tactical considerations. Since the initial tactical packet networking capabilities were developed by the Services to satisfy Service-specific requirements, separate approaches to data security began to evolve within the Services. Thus, the ITSDN program plan identified the need to unify these efforts through an integrated tactical security architecture that would be compatible with the DISN-NT strategic security architecture.

Early data communications experiments were conducted by the US Army at the Army Signal Center in Fort Gordon, Georgia. It soon became apparent that these experiments had the potential to become a basis for a joint test bed activity in which many of the more complex joint networking problems might also be addressed. Thus, the operational impetus of the Army internal data networking requirements, the ITSDN joint requirement, and the emerging goals of the C4I for the Warrior (C4IFTW) Joint Staff initiative became the basis for a series of joint Secure Tactical Data Network (STDN) demonstrations. STDNs would be led by the Services with DISA/JIEO/JITC support and would serve as a means to demonstrate and assess joint C4I data systems interoperability and to identify both procedural and technical solutions to current interoperability problems. Additionally, the demonstrations would allow commercial vendors to show how their products potentially could satisfy C4IFTW needs.

The first three STDN demonstrations (STDN-1 through STDN-3) were conducted at the Army Signal Center, Fort Gordon, Georgia. The Army acted as host in each case. Initially, the focus was only on communications and data network connectivity; however, STDN-3 was broadened to include data systems applications interoperability among the components of a joint task force (JTF).

STDN-4, the fourth in the series of STDN demonstrations, was hosted by the Navy and focused on C4I support for a maritime joint task force operating in the Pacific theater. Actively supported by USCINCPAC, this latest STDN included a broad range of C4I technology demonstrations and undertook serious efforts to implement advanced C4IFTW operational concepts using those technologies.

The STDN-4 demonstration was conducted during August to September 1993. Of special significance was the design and installation of the "Wahiawa Super Gateway" in Hawaii. This gateway was the centerpiece of the architecture that provided data communications connectivity between shore-based command centers (i.e., USCINCPAC and its components) and a deployed JTF and its components via SHF SATCOM. STDN-4 broke new ground in achieving wide area data communications connectivity and also in giving C4IFTW program visibility to the warriors themselves. It was the first of the demonstrations to involve a CINC and the first to use a CINC's force as the JTF. The fact that the JTF was afloat added to the importance of the demonstration. Finally, there was significant participation from all four Services.

138 The section is based on [STDN-4 1993a], STDN-4 1993b], and [Walsh 1994].

The following general results of STDN-4 indicate the breadth of capabilities that were actually shown to work and the expanding level of expertise in the joint C4IFTW community with regard to data networking technology:

- A wide-area joint network of networks was established and data was exchanged among a variety of users operating a variety of systems in a variety of environments.
- A C4I system that supported the PACOM Two-Tier C2 concept was demonstrated.
- A C4I system that provided a maritime JTF advanced information exchange capability over extended distances was demonstrated.
- Warrior information pulls were achieved, most notably in intelligence.
- Useful advanced C2 technologies, such as distributive collaborative planning tools, were demonstrated.

The original purpose of the STDN series of demonstrations was to advance the technical and operational understanding of the participants regarding the interconnection of tactical packet communications networks with strategic long-haul packet networks. The principal means to achieve this purpose has been the actual assemblage, test, and operation of equipment strings in the field using currently fielded or readily available hardware and software. This approach to what is becoming an increasingly complex problem allows Service personnel to get smart quickly on the capabilities of present day technology, to experiment with alternative interconnection means, and to understand early on what inter-networking solutions will and will not work in a tactical environment. The strong emphasis on learning through doing has been the trademark of STDN demonstrations.

More recently, particularly in STDN-4, the scope of activities has increased beyond communications networking. The STDN agenda now includes a full range of C4I technology demonstrations and serious efforts to implement advanced C4IFTW operational concepts using that technology. While there is obviously a strong desire in the C4I community to quickly implement new capabilities that warriors can relate to, there is also a real danger in trying to mix too much new technology with new concepts too fast, especially in a relatively unstructured demonstration environment. The challenge of managing this complex activity under the heretofore ad hoc STDN program appears to be too great. A new demonstration program construct is needed.

Joint Warrior Interoperability Demonstration (JWID). The name "STDN" was originally conceived by the technical community to describe a relatively narrowly focused technical activity. That name no longer accurately describes the broader command and control activity that has evolved and it certainly does not encourage warrior involvement or interest; the new activity name is Joint Warrior Interoperability Demonstration (JWID). The next JWID is planned for 1994. [Ref. Walsh 1994]

19.11.2 US DoD Transition to GOSIP[139]

The US DoD intends to adopt OSI protocols as a full co-standard with DoD protocols, specifically for message handling and file transfer (MIL-STDs 1777, 1778, 1780, and 1781). OSI protocols are expected to "become the sole mandatory interoperable protocol suite." [Ref. ASDC3I 1987] The Defense Communications Agency (DCA) [now the Defense Information Systems Agency (DISA)] has been named as the DoD Executive Agent for Data Communications Protocol Standards, and in June 1988 this agency promulgated an OSI implementation strategy.

139 This section is based on excerpts from [Bryant 1993].

[Ref. DCA 1988] The Services and Agencies have developed transition plans to comply with this strategy.

Although mandated for tactical, strategic, and mission support information systems, DoD's OSI migration efforts have been focused primarily on strategic and mission support systems. DoD established the Defense Message System (DMS) program to migrate from the existing AUTODIN messaging system to X.400-based implementations within strategic and mission support systems. Concurrently, the DoD, through the DMS Program Office, has participated in the allied effort to develop ACP-123 in the strategic world (to replace the commonly used ACP-127 messages). Today's C3I systems rely heavily on the transferring of messages around the tactical environment and between the tactical and strategic environment.

Although one of the most extensive and pervasive OSI-based programs, DMS is not the only OSI user within DoD. The Defense Information System Network (DISN) is also migrating to OSI support. The DISN routers currently support both the Internet Protocol (IP) and the OSI-based connectionless-mode network protocol (CLNP). Additionally, an SMTP-to-X.400 application gateways exists to connect TCP/IP-based users to OSI-based users. DoD recently approved a DoD standardized profile (DSP) based on the X.400 ISP and the NATO standardized profile (NSP) for military messages, as DoD MIL-STD-2045-17501. DSPs for specific X.400 content types are also being developed.

Rapidly deployable forces require joint (and combined) connectivity from military commanders at the level of CINCs and Joint Task Forces (JTFs) and military staff at the level of the US DoD Joint Staff. Technology allows national intelligence assets to distribute products directly to battlefield commanders. However, many people remain skeptical about the ability of OSI-based protocols and products to operate in the noisy, bandwidth-limited, closed environment of the tactical user. Specific concerns include the following:

- Amount of achievable information throughput given the overhead normally associated with OSI protocols and the narrow bandwidths associated with tactical circuits
- Ability to operate in a simplex mode to support emission control requirements
- Lack of security services to ensure data confidentiality, data integrity, and non-repudiation of sender and receiver
- Ability to operate near-real-time networks
- Ability to internetwork with existing tactical systems.

19.11.3 US Corporate Information Management

The US DoD has initiated a major effort to transition the DoD's present information systems and associated information technology resources to a communications and computing infrastructure based on the principles of open systems architecture and systems transparency. The breadth of this work is for DoD-wide corporate information management (CIM) and includes in its scope both tactical and strategic CCISs. A summary of the CIM assessment of the standards availability is given in Table 73. The column on standards status indicates whether adequate standards are now or in the future available for each service and if not, whether there is a gap (some but not sufficient standards) or a void (no standards). The table further shows the dates at which US federal standards (FIPSs) are expected.

Table 73. US DoD (CIM) Assessment of Standards Availability

SERVICE AREAS	SERVICE	STANDARDS STATUS	CIM	TIMEFRAME FOR STANDARDS AVAILABILITY: 1 OCT 1992	1 OCT 1993	1 OCT 1994	1 OCT 1995
Operating System	Kernel	Now	●	FIPS Pub 151-1 (POSIX)	FIPS Pub 151-2		
	Shell and Utilities	Now	●	IEEE P1003.2	FIPS Addition		
	Realtime Extension	Future	●	IEEE P1003.4	FIPS Addition		
	Security	Future	●	IEEE P1003.6 (Draft Standard)	Approved IEEE Standard	FIPS Addition	
	System Management	Future	●	Draft Government Network Management Profile (GNMP) FIPS	Approved FIPS Supplanted by MIL-STD-2045-38000		
Programming	Programming Languages	Now	●	FIPS Pub 119 - Ada		FIPS Pub 119-1 (Ada-9X)	
	Case Tools and Environment	Now		ECMA Portable Common Tool Environment (PCTE) Specification 149			
	Security	Void					
User Interface	Client Server Operations	Now	●	FIPS Pub 158 (X Window System)			
	Object Definition and Management	Now		DoD Human Computer Interface Style Guide			
	Window Management	Now	●	FIPS Pub 158 (X Window System)			
	Dialogue Support	Future	●	Future Standard - IEEE P1201.X	Final Draft - IEEE P1201.X	FIPS 158 Addition	
	Security	Void					
Data Management	Data Dictionary - Directory	Now	●	FIPS Pub 156 (IRDS)			
	Data Management	Now	●	FIPS Pub 127-1 (SQL)		FIPS Pub 127-2 (SQL +)	FIPS Pub 127-3 (SQL++)
	Distributed Data	Future	●	Draft ISO Standard - Remote Database Access (RDA)	Final ISO Standard	FIPS Addition	
	Security	Now	●	NCSC-TG-021 (TDI)			

Key: ● Included in September 1992 DoD Profile of Standards.

Source: *Technical Reference Model for Information Management*, Version 1.3, Coordination Draft, Center for Information Management, DISA, 30 September 1992, UNCLASSIFIED.

Table 73. (Continued)

SERVICE AREAS	SERVICE	STANDARDS STATUS	CIM	TIMEFRAME FOR STANDARDS AVAILABILITY 1 OCT 1992	1 OCT 1993	1 OCT 1994	1 OCT 1995
Data Interchange	Document Interchange	Future	●	Planned FIPS Pub (Office Document Architecture/ Office Document Interchange Format/Office Document Language ODA/ODIF/ODL)			
	Document Interchange	Now	●	FIPS Pub 152 (SGML)			
	Vector Graphics Data	Now	●	FIPS Pub 128 (CGM)			
	Raster Graphics Data	Now	●	FIPS Pub 150 (Type 1)			
			●	Planned FIPS Pub (Type II)	Draft FIPS	Final FIPS	
	Product Data Interchange	Gap	●	Planned FIPS Pub (Initial Graphic Exchange Specification/IGES)	Draft FIPS	Final FIPS	
	Product Data Interchange	Future		Draft International Standard (Standard for the Exchange of Product Model Data - Step)	Final ISO Standard	Draft FIPS	Final FIPS
	Electronic Data Interchange	Now	●	FIPS 161 - Effective 30 Sept 1991		Convergence of X.12 and Edifact	
	Security	Void					
Graphic Services	Graphics	Now	●	FIPS Pub 120-1 (GKS)			
	Graphics	Now	●	FIPS Pub 153 (PHIGS)			
	Security	Void					

Key: ● Included in September 1992 DoD Profile of Standards.

Source: *Technical Reference Model for Information Management*, Version 1.3, Coordination Draft, Center for Information Management, DISA, 30 September 1992, UNCLASSIFIED.

Table 73. (Continued)

				TIMEFRAME FOR STANDARDS AVAILABILITY			
SERVICE AREAS	SERVICE	STANDARDS STATUS	CIM	1 OCT 1992	1 OCT 1993	1 OCT 1994	1 OCT 1995
Network Services	Data Communications	Now	●	FIPS Pub 146-1 (GOSIP)		FIPS Pub 146-2 (GOSIP)	
	Telecommunications	Now	●	MIL-STD-187-700			
	Transparent File Access	Future		Draft IEEE Standard P1003.8	Final IEEE Standard	Approved FIPS	
	Personal/Micro Computer Support	Void					
	Distributed Computing	Future		Draft OSF Specification (NCS/RPC)	Draft FIPS		Final FIPS
	Security	Now	●	ISO 7498-2			
	Security	Now	●	NCSC-TG-005 (TNI)			
	Security	Future	●	Draft IEEE Standard 802.10		Addition to FIPS 146	
	Security	Gap		DNSIX, Version 2.1		MaxSIX	
	Security	Future	●	Draft ISO Standard for Transport Layer Security Protocol (TLSP)	Final ISO Standard		
	Security	Future	●	ISO Committee Draft for Network Layer Security Protocol (NLSP)	Draft ISO Standard for NLSP	Final ISO Standard	
Security	Evaluation Criteria	Now	●	DoD 5200.28-STD		Revision Planned	
	Compartmented Mode Workstation	Now	●	DRS-2600-5502-87			
	Compartmented Mode Workstation Evaluation Criteria	Now	●	DRS-2600-6243-91, Version 1			
	Compartmented Mode Workstation Labeling: Encoding Format	Now	●	DDS-2600-6216-91			
	Compartmented Mode Workstation Labeling: Source Code and User Interface Guidelines	Now	●	DDS-2600-6215-91			
	Digital Signature	Future	●	Draft FIPS Pub (DSS)			

Key: ● Included in September 1992 DoD Profile of Standards.

Source: *Technical Reference Model for Information Management*, Version 1.3, Coordination Draft, Center for Information Management, DISA, 30 September 1992, UNCLASSIFIED.

19.11.4 DoD-Wide and Multi-Service Architectures and Environments

DoD Integrated Communications Architecture. The Defense Information Systems Agency (DISA) and the military Departments are formulating information and security architectures for an Integrated Communications Architecture (ICA), concerned with platform, base-level, and long-haul communications. These architectures are expected to be founded on local ISDN switches and high-speed LANs; the long-haul networks will also provide ISDN service. In security, new technology for end-to-end and multi-level security devices is being exploited. [Ref. COPERNICUS 1991]

Global Command and Control System (GCCS) Common Operating Environment (COE).[140] In 1993, the US Joint Staff began work on the GCCS with two objectives: replacement of the Worldwide Military Command and Control System (WWMCCS) and implementation of the C4I For the Warrior concept. GCCS is planned to improve the joint warfighter's ability to manage and execute humanitarian, crisis, and contingency operations and provide a means for integration of the Service C4I systems. It covers the spectrum of conflicts from routine peacetime operations to non-nuclear strategic war. The concept builds upon lessons learned from previous conflicts, operational requirements, the effects of rapidly changing technology, and the direction of a changing national security strategy. GCCS will become the single C4I system to support the war fighter, whether from a fox hole or from a command post. The GCCS will provide a single view of the military C4I for the joint war fighter. The view will be through a widely distributed, user driven network to which the war fighter "plugs in."

In the past, grand design acquisition strategies often failed in the command and control (C2) arena. Large-scale acquisitions typically take years to scope and award. Technology insertion is difficult to accomplish, failing to take advantage of technical advances and price reductions. The GCCS programs break with this model of development. They plan to pursue an evolutionary migration strategy that:

- Keeps the war fighter involved at all levels
- Allows the war fighter to retrieve, manipulate, share, and view database information as needs change
- Provides a unifying architecture that provides a path for migration
- Builds an open infrastructure flexible enough to easily accommodate future requirements
- Relies upon the services as GCCS components, data sources, and information sources
- Provides the vehicle for technology insertion.

As stated in the Technical Architecture for Information Management (TAFIM) [Ref. TAFIM 1993, Volume 3], the following guidelines apply to the design of the GCCS COE:

- An architecture is a set of components and a specification of how these components are connected to meet the overall requirements of an information system.
- The components of an architecture provide implementations of the reference model services relevant to a specific system.
- An architecture will contain components to implement only those reference model services that it requires.

---

140 Based on *GCCS Common Operating Environment* [DISA 1994].

- Components may implement one, more than one, or only part of a service identified in the reference model.
- The components should conform to the profile standards that are relevant to the services they do implement.

The following are assumptions related to the GCCS COE:

- The COE is to migrate to eventual compliance with the TAFIM, Volume 3 and the technical reference model (TRM) contained in Volume 2 of the TAFIM.
- Non-developmental items (NDIs), including both commercial off-the-shelf (COTS) and government off-the-shelf (GOTS), are the preferred implementation approach.

Standards and products being considered for the near-term version of GCCS COE are shown in Figure 39.

The GCCS mission area applications reside at the top of the DoD Technical Reference Model. Although lower layers often provide services that are useful in themselves, the principal purpose of the lower layers is to support the mission area applications.

The GCCS mission area applications will tend to be custom developed and targeted to a specific function or user community. Mission area applications can build upon the services offered by other mission area applications, support applications and platform services, and exchange and make use of information in other mission area applications. However, mission area applications that offer shared functions to be used by a variety of other applications can be considered for inclusion as a support application.

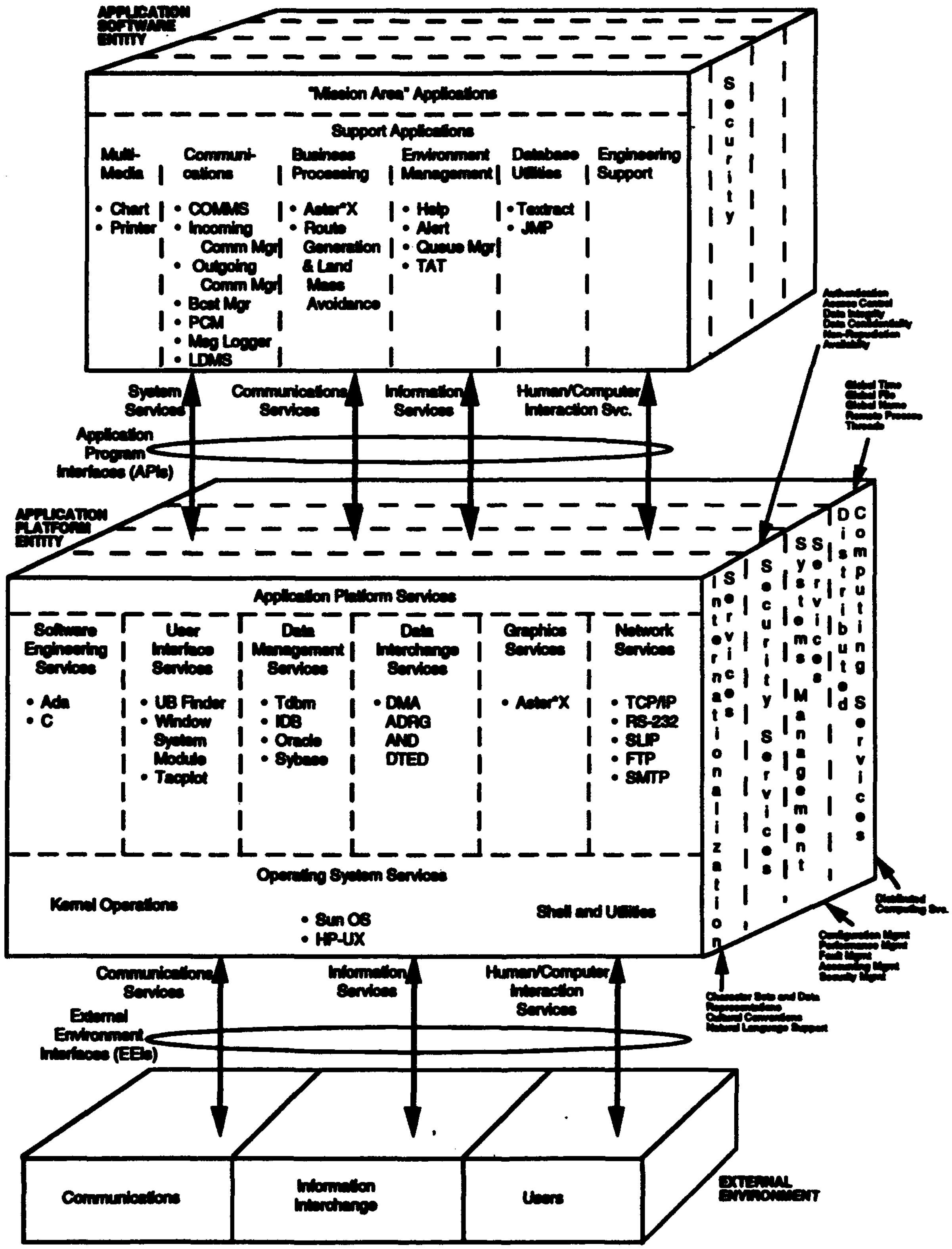
The GCCS mission area applications can be one or a combination of the following:

- Candidate applications developed by the Services; i.e., GOTS
- Candidate applications developed by the Services, which are modified for use in the GCCS
- Applications custom developed for the GCCS
- COTS.

The preliminary definition of the GCCS Block 1 is the following:

- Technical Insertion Program (TIP) [which includes Joint Flow and Analysis System for Transportation (JFAST), Logistics Sustainment Analysis and Feasibility Estimator (LOGSAFE), Force Augmentation Planning and Execution System (FAPES), and Dynamic Analysis and Replanning Tool (DART)]
- Unified Build (UB)/Ocean Surveillance System (OSS)
- GCCS Status of Resources and Training Systems (GSORTS)
- Contingency Tactical Air Control System (TACS) Automated Planning System (CTAPS) module for Air Tasking Order (ATO)
- USCINCEUR Command Center System (UCCS).

GCCS support applications can provide services that are useful without need for a mission area application. However, the support applications are intended to be building blocks for the mission area applications. According to the TAFIM, there are two types of support applications: programs and reusable software components. The programs can be loaded and executed. These programs offer a service to other support applications and to mission area applications. The reusable software components cannot be loaded and executed themselves. These components are incorporated into mission area and support applications. Both types of support applications provide common functions available through documented interfaces.



Source: [DISA 1994].

Figure 39. Near-Term GCCS COE

The GCCS support applications that are executable include COTS and GOTS and will be shared by one or more mission area or support applications. Examples of common COTS support applications are word processing, transaction processing, screen generation, E-mail, and spreadsheets. Examples of GOTS support applications are audit trail, queue manager, and alert manager. The support applications that are reusable software components are primarily GOTS, although there is no technical reason preventing use of reusable COTS components.

Multi-Service Common Operating Environment. The US Army, Navy, Marine Corps, and Air Force agreed in 1991 on a Common Operating Environment (COE) based, in part, on US GOSIP and the NIST APP/OSE.[141] The goal of the COE is to reach consensus among the Services as a means of promoting interoperability, portability of applications, and the sharing of ideas, software, and data products. The COE addresses, in part, the growing interdependence among federal organizations; critical need for common architectures, communications networks, and databases; excessive dependence on single vendors; and underdeveloped interoperability of products and portability of people, data, and applications. Anticipated benefits are improved efficiency of Service systems in supporting deployed commanders, reduced costs by cutting development and fielding time, reduced porting effort, improved interoperability between systems, reduced training time, reduced duplication of effort between Services, improved system capabilities, and reduced maintenance efforts.

The COE is a suite of standards agreed to by a consensus of participants. The standards will be commercial standards where possible to further reduce the cost of developing software. The elements of the environment to be addressed, eventually, by the COE standards include the following:

- Open system hardware architecture
- Data architecture
- Software documentation
- LAN/BUS interfaces
- Programming language
- Operating system
- Human-machine interface
- Graphics interface
- Map and overlay display
- Real-time track database management services
- Encyclopedic database management services
- Security services.

The COE Working Group has agreed to commonality in the following areas: POSIX compliance (FIPS-151); Ada; Ada-to-C bindings for a relational database management system (DBMS), X-Windows, and UNIX; X-Windows 11.2 migrating to PEX; Motif as the graphic user interface (GUI); SQL and its evolutions; and TCP/IP evolving to GOSIP for network services. The Services are now actively seeking a description of common requirements for system architectures and system specifications. They are seeking agreements on recommendations for a common style guide, standard interprocess communications, standard map data, standard graphic

141 The Air Force, Coast Guard, Defense Intelligence Agency, Defense Mapping Agency, JIEO, and the Joint Staff are all represented in COE discussions.

user interface, standard relational DBMS-to-SQL interface, and a standard map display. Table 74 identifies the services for the COE and (in the second column) example standards (the latter are taken from the Navy's implementation). [Ref. COE 1991]

Table 74. US Multi-Service Common Operating Environment

SERVICES	EXAMPLE STANDARDS
System Support	
Operating systems	UNIX–POSIX compliant
Communications interface & protocols	GOSIP, TCP/IP, SAFENET, CSS
Windowing (human-machine interface)	X-Windows II (Release 4)
Systems administration	Diagnostics
System management	CMIS, CMIP, SNMP
System security	COMPUSEC Orange Book, SDNS
BUS architecture	VME, FUTUREBUS+
C2 Support	
Display toolkit	Motif
Database manager	SQL, Relational DBMS
Internal interface	BTR
System services	Ada, C, Ada bindings
Display	Chart+
C2 Communications Applications	
External communications	GLOBIXSs, TADIXSs, Physical nets
Message processing	US Message Text Formats, OTH-G, TADILs A & B, Bit-oriented messages
Correlation	Attributes, ELINT, Probabilistic, Acoustic
Database	Track, C&P/008

Source: *Fleet Communications in the Copernicus Architecture*, Final Draft, 20 June 1991, UNCLASSIFIED.

The top-level architecture model will be the DoD Technical Reference Model (see Section 1.3 above), and a combination of the style guides for the DoD Intelligence Information Systems (DODIIS) will be considered as the DoD human computer interface style guide. The SQL-Ada Module Description Language (SAMeDL) has been recommended for DBMS-SQL interface (and is used for US Marine Corps Common Application Support Software inter-module communication).

SPACECOM Assured Mission Support Space Architecture (AMSSA). Space Command (SPACECOM) has developed the AMSSA to consolidate several architectures and expand them to all elements of air-land-sea forces. The goal is to integrate the use of space-based satellites with the communications requirements of the operational forces. The AMSSA seeks to apply "architectural-level" interoperability standards across communications; navigation; environmental monitoring; intelligence; surveillance; mapping, charting, and geodesy (MCG); launch; C2; satellite control; and logistics functional areas in support of the tactical user. The architecture seeks standards in the following six service areas with the associated functions and characteristics:

- Communications: switching, frequency, data rate, wave form
- Navigation: geolocation, timing, velocity
- Launch: mix-and-match flexibility and intercompatibility
- Integrated satellite control services (ISCS): satellite control, mission data processing, protected links
- Integrated logistics support (ILS): supportable, maintainable, operable
- Command and control: unity of command, survivable.

Standards are to be open, modular, and backward compatible without dictating particular engineering solutions. [Ref. SPACECOM 1991]

Defense-Wide Common Security Architecture. One of the tasks in the Defense-Wide Information Systems Security Program (DISSP), which is being conducted by DISA and the National Security Agency, is the development of a Defense-Wide Common Security Architecture. This architecture will include information systems security standards and protocols, uniform security accreditation procedures, security technology, and a transition plan. The architecture's scope includes: guidelines for system design, applicability to many information systems, addressing systems in detail at the service level, identifying relevant technology, describing relevant technologies and important issues, ensuring interoperability, and focusing on cost effectiveness. It is intended to support the increased use of multi-level security in DoD systems. [Ref. DISSP 1991]

C2 Architecture for SDIO Segments. The Strategic Defense Initiative Office (SDIO) has issued a Fixed/Mobile Segment (FMS) Standard to be used in the design of all fixed and mobile ground segments for the Strategic Defense System (SDS). Such segments include the Ballistic Missile Defense Command Center, the Service Component Command Center, the Regional Operations Centers, the Element Operations Centers, and the Ground Entry Points. This document covers open hardware and software architecture and software and user environments. Standards prescribed in the FMS document include [Ref. SDIO 1991]:

- Electrical interfaces: RS-232, RS-422/423, RS-449, IEEE 488.1/.2, MIL-STD-1881-114 or MIL-STD-188, ISO 8802.3 or ANSI X3T9.5 (Fiber Distributed Data Interface), and MIL-STD-1553 (data bus).
- Backplanes: Versa Module Europe bus (VMEbus) (IEEE P1014) or VME Extension for Instrumentation (VXIbus, IEEE P1155). The selection of VMEbus is to provide future growth to FUTURbus (IEEE 896.1). This may require a VMEbus-to-FUTURbus bridge compliant with IEEE P1014.2.
- Protocols: TCP/IP (MIL-STD-1788 and MIL STD-1777) or as available GOSIP (FIPS-146)-compliant protocols.
- Human-computer interface (HCI): X-Window System implementation (FIPS-158) of OSF/Motif featuring the direct manipulation of windows, icons, data, menus, and objects within the windows (primarily a "point-and-click" system of direct manipulation that minimizes typing. HCI complies with MIL-STD-1472 except where there are conflicts with OSF/Motif, Motif Style Guide, and multiprocessor requirements.
- Software: Includes the NIST Application Portability Profile (FIPS-151), GOSIP protocols and services in all software for SDS C2 ground segments, Ada for all software development (with some C programming permitted), POSIX-compliant operating systems, database-defined constants (parameters), database management system supporting an SQL interface.
- Information processing system security: level of multi-level security protection is TBD. Underlying operating system in the applications processors meets DoD 5200.28-STD for controlled access protection (class C2).

19.11.5 US Defense Data Network (DDN)

Packet Switching for DDN. The US Defense Communications Agency has implemented an X.25 packet-switched protocol for the Defense Data Network (DDN). This protocol includes the use of the US DoD-unique protocols for Layers 3 and 4, namely the Internet

Protocol (IP) and the Transmission Control Protocol (TCP). DDN supports over 50,000 users of a DoD-unique electronic mail (E-Mail). DDN contains a set of physically, procedurally, and cryptographically secured packet switching segments for classified E-Mail in the Defense Integrated Secure Network (DSNET) (e.g., DSNET-1, DSNET-2, DSNET-3). There are additional segments for unclassified E-Mail [e.g., Military Network (MILNET) and Advanced Research Projects Agency Network (ARPANET)]. Local area networks (LANs) are connected to the DDN by gateways or hosts using the DoD IP.

Defense Message System (DMS)—Upgrades for DDN. The US has initiated [Ref. DCA 1989c; MROC 3-88 1989] a project called the Defense Message System (DMS) that will eventually integrate DDN with the Automatic Digital Network (AUTODIN). DMS will phase in [Ref. DCA 1988a] such protocols and services as US GOSIP, ITU-TS X.400 Message Handling System, High-Level Data Link Control (HDLC) for subscribers, new asynchronous protocol(s) with reliable transfer for subscribers, and ITU-TS X.500 Directory Services. TCP/IP protocols will be phased out. Initially (Phase I) a US DoD-unique security program called BLACKER will be implemented at the host-to-host level, which will ultimately result in an integrated DSNET. Later (1993) DDN will consist of MILNET (unclassified) segments and DSNET (classified) segments connected by BLACKER-protected gateways.

The following general requirements have been validated by the DMS Multicommand Required Operational Capability (MROC) in 1988:

- Connectivity and interoperability
- Guaranteed delivery and accountability
- Timely delivery
- Confidentiality and security
- Sender authentication
- Integrity
- Survivability
- Availability and reliability
- Ease of use
- Identification of recipients
- Message preparation support
- Store and retrieval support
- Distribution determination and delivery.

In November 1991, DISA prepared a draft DMS Required Operational Messaging Characteristics (ROMC) document to specify the messaging characteristics that are derived from the 13 general requirements identified above. The ROMC is solution independent and develops quantitative characteristics based on baseline DMS requirements and from engineering estimates. [Ref. DISA 1991]

An OSI Transition Plan has been prepared for the DMS. The April 1991 draft of this plan defines transition goals, constraints, activities, dependencies, and schedule for the transition of the DMS to an architecture and supporting environment that employs the US GOSIP. It documents the activities necessary to transition DMS hardware and software components, protocols, formats, and procedures to an OSI-based capability, while providing for interoperability between the baseline capability and the OSI-based capability during the transition period.

Beginning with the Baseline in 1989, the plan identifies three transition phase (1990-94, 1995-2000, and 2001-2008). The major capabilities and changes included in the plan are X.400 messaging, X.500 Directory Services, management capability, AUTODIN-to-DDN interconnectivity, Allied interoperability, tactical interoperability, and AUTODIN phase out. Phase I augments the 1989 Baseline with initiatives to bridge the gap between AUTODIN and the DDN and to improve base-level automation.

Phase II will include X.400/X.500 individual and organizational messaging with the SDNS Message Security Protocol (MSP) protection (vice distinct AUTODIN and E-Mail in the first phase). The Base Information Transfer System (BITS) will begin to be deployed at the base level in Phase II. Most but not all of the Baseline and Phase I components will be phased out. This evolution continues and is completed in Phase III. [Ref. MITRE 1991]

Defense Message System (DMS).[142] The US DoD is fielding a highly distributed and integrated directory service based on the ITU-TS X.500 and ISO/IEC 9594 Directory Specifications. The first application to be served by the directory will be the Defense Message System, which is based on the CCITT X.400/ISO/IEC 10021 messaging standard. This directory service will replace several other directories: the paper directories of the Automatic Digital Network (AUTODIN) and the WHOIS directory on the DoD Internet. The DMS directory is expected to evolve to a DoD-wide Directory and will be used to support other network and application services. Comprehensive directory services are essential to assist users in finding resources, including X.400 user addresses. The Directory enables such queries to be made in a logical fashion much like looking up a person's name in the telephone directory to find his or her telephone number.

The target architecture for DMS is based on the 1993 edition of the CCITT X.500 and ISO/IEC 9594 Directory specifications, the 1988 CCITT X.400 and 1990 ISO 10021 messaging standard, MSP, STANAG 4406, and ACP 123. MSP was developed as a cooperative project between government and industry under the sponsorship of NSA. MSP provides confidentiality, data origin authentication, integrity, access control, for messaging, non-repudiation with proof of origin, and non-repudiation with proof of delivery.

The X.500 Directory consists of a distributed network of DSAs that collectively contain information about real-world objects in the Directory Information Base (DIB). Each DSA has knowledge of at least one other DSA as a source of information that the first DSA does not contain. The Directory is queried by Directory User Agents (DUAs), the access interface for directory users that may be a person or a computer program. Generally, only a Directory administrator will have a DUA that is permitted to update user and operational information—such as access control information—while other users may have limited access.

The current DoD policy is for all X.400 users to have the P772 content type supported by their user agents. The P772 content type adds military extensions to the standard P22 content type. ACP 123, which replaces ACP 127, specifies X.400 profiles and procedures. (ACP 127 specifies the message format now used by US allies.)

DMS has worked in national and international directory groups to add access control, replication, and systems management to the Directory. The final meeting for the 1993 edition of the Directory Specifications was held in October 1992. The text is collaborative and has been

142 This section is based on excerpts from [Gardner 1993].

approved by ISO; when the text has been approved by CCITT, it will be published. In the meantime, editor's text is available from the ISO Rapporteur. Features added in 1993 include the features needed by DMS, and products supporting these new features are expected soon.

Enhancements to the X.400 and X.500 standards are needed in order to standardize several key features for the Directory in commercial off-the-shelf products. Among the enhancements to the standards are the following:

- Enforcement of consistency between aliases and the entries to which they correspond
- Management of directory services and the system components that underlie them
- Rule-based, administratively imposed access control in the X.500 Directory standard
- Changes to the X.400 standard to allow capability information to be stored with each originator/recipient address
- Standardization of X.400 static routing information to be stored in the Directory
- Confidentiality of directory information.

US DoD Tactical Packet Switching Systems. The following summarizes the packet switching systems employed by the Services for tactical applications [Ref. Pennington 1993]:

- The Army's Mobile Subscriber Equipment (MSE) Tactical Packet Network (TPN) overlay will provide an in-theater data communications capability for command and control. The TPN uses X.25 packet switch technology and DoD protocols. Fielding began in FY92.
- The Air Force Tactical Secure Data Communications (TASDAC) system will provide secure data transmission among forward and deployed Air force units and fixed base parent organizations. The TASDAC system will attach workstations over 802.3 LANs, and use COTS IP routers as external interfaces. TASDAC will implement DoD protocols, with provisions for evolution to GOSIP in the future. Fielding was projected to start in FY93.
- The Navy's Copernicus architecture defines Navy command, control, communications, and computer systems. This architecture will be implemented beginning in FY93, and will revolutionize information exchange in the shore and afloat environments. One important emphasis of Copernicus is to move away from traditional Navy stove-pipe systems. An initial capability may include shipboard routers.
- The Marine Corps Tactical Communications Distribution Node (TCDN) will provide a front–end capability for resolution of protocol differences between Marine and other Service systems. The Marine Corps uses proprietary LANs for data distribution, attaching host systems only (not workstations). A COTS IP router is presented as the external interface.

19.11.6 Support for C4I for the Warrior

The US Joint Staff (J6J) has developed a concept to intelligently and uniformly apply information technology to facilitate the command, control, communications, computers, and intelligence (C4I) support to the warrior. The concept is standards based and focuses on exchange of information between existing C4I systems. Briefly, the capability of this concept is described as "a fused, real-time, ground truth picture of the warrior's battle space and the ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute the warfighting mission in the battle space." Each step of the interoperability transition process would involve the warrior with the technicians to ensure the result is what is really needed. Following

refinement of the concept, the next step is development of a joint interoperability architecture. This architecture would fashion the Service architectural concepts (some are discussed below) into an integrated whole, coordinated with the CIM initiatives. The standardization underlying the architecture would specify services in the form of a joint interoperability standard for the common interfaces. Included in the concept is a "database in the ether, which would have common access protocols and make it unnecessary for the user to have knowledge of the physical location or nature of distribution of the information elements being accessed." [Ref. J6J 1991]

19.11.7 Service Architectures and Standards

ATCCS Architecture. The Army Tactical Command and Control System (ATCCS) is the US Army's tactical system-of-systems concept. As shown in Figure 40, the tactical systems are grouped into five battlefield functional areas (BFAs): maneuver control, fire support, air defense, intelligence and electronic warfare (IEW), and combat service support (CSS).

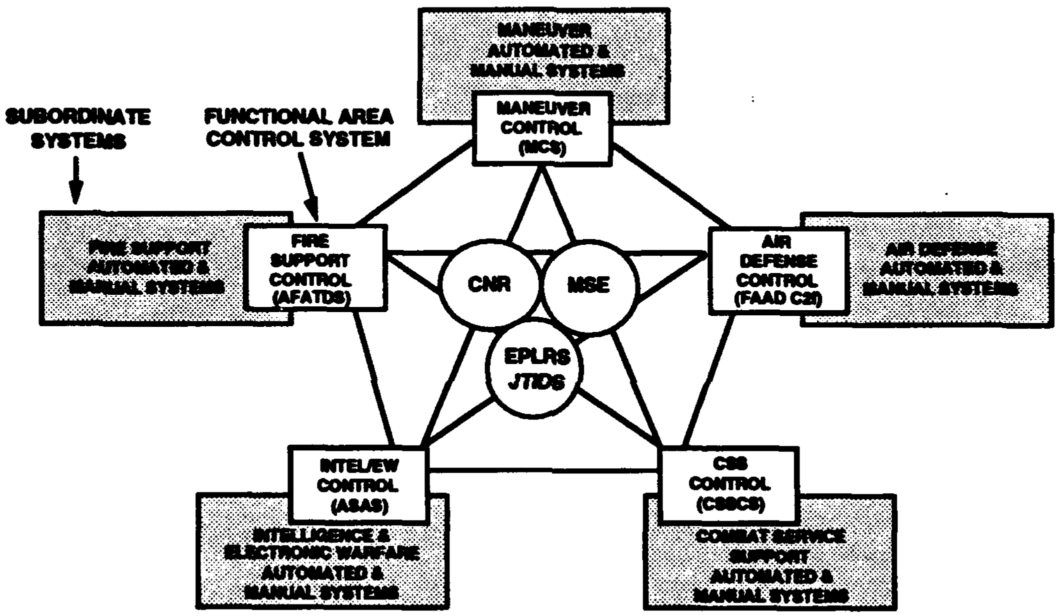


Figure 40. US Army Tactical Command and Control System (ATCCS)

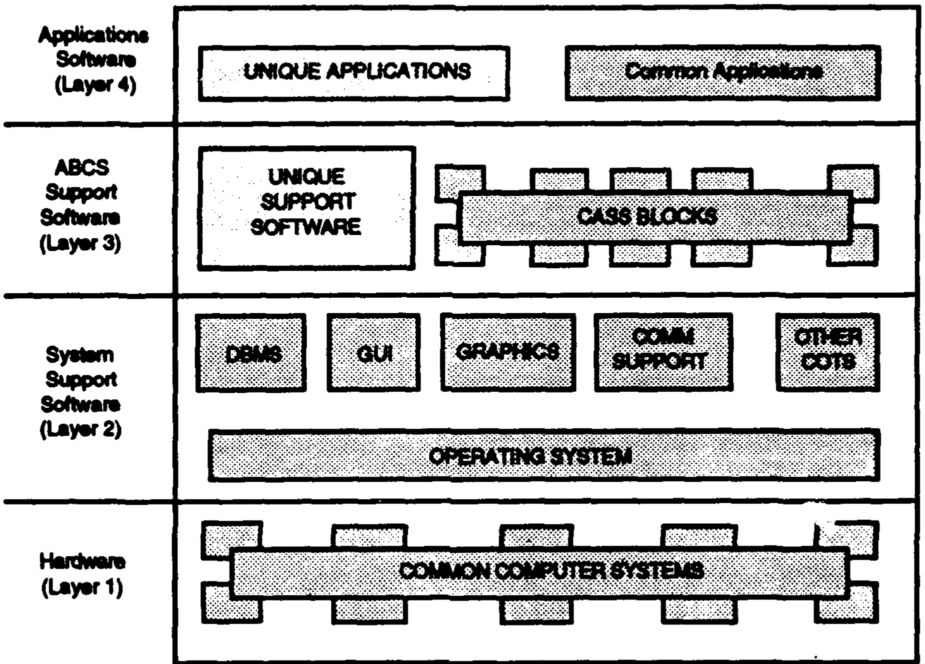
Each functional area for the US Army is planned to have a single BFA control system and a number of subordinate automated and manual BFA systems. The objective control systems are [Ref. Levine 1994a]:

- Maneuver Control System (MCS). MCS quickly and accurately moves tactical information on the battlefield, allowing a commander to readily access information and display current situation reports, intelligence and contact reports that assess enemy strength and movement, as well as provide status of friendly forces. MCS then aids the battle staff in rapidly disseminating the commander's orders. MCS has been fielded on militarized hardware called the Tactical Computer Terminal (TCT) and nondevelopmental item computers called the Tactical Computer Processors (TCP). Fielding with the ATCCS Common Hardware Software (CHS) is planned with the next version (V12), planned for FY95.
- Advanced Field Artillery Tactical Data System (AFATDS). AFATDS is a totally integrated fire support command and control system. It will process fire mission and other related information to coordinate and maximize the use of all fire support assets,

including mortars, field artillery, cannon, missile, attack helicopters, air support, naval gunfire, and offensive electronic warfare. AFATDS will provide processing capabilities from corps to the forward observer. AFATDS completed concept evaluation (CE) in 1989 and began full-scale development in 1990. When fielded with ATCCS CHS beginning in FY94, AFATDS will replace the Tactical Fire Direction System (TACFIRE) now being used in the heavy divisions, and the Lightweight TACFIRE (LTACFIRE) now being fielded to the light divisions.

- Forward Area Air Defense (FAAD) Command, Control, and Information (C2I). FAAD is an integrated system of weapons, sensors, and C2. It protects maneuver forces, critical command posts, and combat support and combat service support elements from low-altitude air attack. FAAD C2I is the element that provides air defense C2 and targeting information to weapons systems. FAAD C2I is a tactical data system being developed with ATCCS CHS that will develop and distribute a low-altitude air defense (LAAD) air picture and C2 information across a division front. Its IOC is planned for FY94.
- All Source Analysis System (ASAS). The ASAS is a ground-based, mobile intelligence processing system designed to provide automated support to the combat commander in the areas of intelligence and collections management; all-source, target, and situation analysis; single and multi-source processing and reporting; electronic warfare; and operational security, as well as support to the generation of intelligence products in those areas. ASAS is an evolutionary development effort consisting of three blocks designed to produce an automated battlefield intelligence fusion system that fully satisfies Army operational requirements. Elements of ASAS will provide seamless support to warfighters at echelons from echelons above corps (EAC) to brigade level. At the corps and division levels, ASAS will operate at the Analysis and Control Element. Sanitized intelligence reports and products will be available from the collateral-level ASAS. At EAC, ASAS will be tailored to meet unique theater requirements. At the maneuver brigade and battalion level, ASAS collateral workstations will be employed. ASAS was developed in the Joint Tactical Fusion program with the Air Force, whose system was called Enemy Situation Correlation Element (ENSCE). When fielded, ASAS will replace the Technical Control and Analysis Center (TCAC, AN/TSQ-130) that is being used in some heavy divisions in the United States and in Europe.
- Combat Service Support Control System (CSSCS). CSSCS will provide a tactical interface to CSS systems deployed to the Continental United States, used in garrison, and fielded for tactical employment. IOC with ATCCS CHS is planned for FY94.

Army Common Operating Environment (ACOE). The ACOE, shown in Figure 41, is based on a four-layer architecture that tracks to the National Institute of Standards and Technology (NIST) Applications Portability Profile (APP) and the DISA Technical Architecture Framework for Information Management (TAFIM) architectures. The four layers consist of: Layer 1 (Common Hardware); Layer 2 (Common System Support Software); Layer 3 [Common Army Battle Command System (ABCS) Support Software (CASS), formerly Common Army Command and Control System (ACCS) Support Software]; and Layer 4 (Common Application Software). Each layer isolates the functionality and interfaces from the other layers. The ACOE fully supports a domain-specific architecture and a centric, systematic reuse program that implements the DoD Software Reuse Vision and Strategy. This ACOE architecture enhances the maintainability of all Army command and control systems, promotes product independence, protects Battlefield Functional Area (BFA) applications programs from commercial-off-the-shelf software changes, and enhances application portability. [Ref. Levine 1994b]



Source: [Levine 1994b].

Figure 41. US Army Common Operating Environment (ACOE)

The ACOE Layer 1 (Hardware) includes computers, displays, printers, facsimile, scanner, LANs, storage devices, special-purpose devices, and tactical communications interface module (TCIM). Protocols provided by the TCIM are specified in Appendix C. [Ref. Levine 1994b]

Layer 2 (System Support Software) of the ACOE comprises the following [Ref. Levine 1994b]:

- Operating system: POSIX-compliant at C2/B1 level with DOS emulation
- Data management: SQL, IRDS, relational DBMS at C2/B1 level
- Graphical user interface: Motif, DoD HCI Style Guide, X-Windows
- Graphics: GKS, PHIGS, PHIGS Extensions for X-Windows (PEX)
- Communications support: GOSIP, TCP/IP, SGML, SMTP, CGM, SNMP
- Other: word processor, spreadsheet, Ada, C, business software packages.

The key component of the ACOE is Layer 3 (CASS). It serves as the interface between the COTS Software and the Applications (common and unique) software. CASS is fully modular Ada-based software. Version 1.2 will be ready for incorporation into ABCS in May 1994. A key portion of the CASS layer is the Message Handling Block, which contains a fully automated, modular Common ABCS Message Parser (CAMP). CAMP support is fully compliant with the Joint Interoperability USMTF standard and is designed to accept updates to the latest Joint message interoperability requirements directly from the DISA/JIEO database rapidly and at minimal cost. The CAMP also supports more efficient data transfer mechanisms such as bit-oriented messages (BOM) and direct transaction-based database element transfers. The CAMP is essential to ABCS since it provides the functions of autofill (from the database) and autoparse (into the database) of information elements critical to meeting system performance requirements. The CAMP is presently

undergoing preparation for Joint Certification and, on successful completion, it will be placed in the Joint software repository and offered to all of the Services. [Ref. Levine 1994b]

CASS has two sublayers: a lower sublayer (Services) to provide the interface to COTS software and hardware and an upper sublayer (Functions) to provide the support software interface to applications. CAMP is an example of a Function. Others are Alert, which captures, queues, processes, and displays audio/visual alerts; Map, which generates, displays, and updates map data; Network Management, which manages and configures network-related parameters; and Workstation Management, which manages and controls workstation functions including the configuration parameters. The Service Sublayer comprises the following: Display Services, which provide lower-level objects for controlling the interactive display using X-Windows and Motif and which control and manage display objects, menus, and windows; DBMS Services, which perform database distribution and replication and which interface the C2 applications to the common database management system; Communication Services, which support the transparent communication between software units across the network; and Operating System Services, which interface C2 applications to the UNIX operating system and which provide file, library, security, and diagnostic services. [Ref. Levine 1994b]

In addition to CASS, many common requirements are being addressed through the development of common applications. The initial common applications being developed are the following [Ref. Levine 1994b]:

- Terrain Evaluation Module (TEM)—Provides each system the ability to view maps, generate overlays, have three-dimensional visualization of terrain, show intervisibility, and other similar map and terrain related functions. It automates the creation, modification, display, and use of overlays combined with raster- or vector-format maps in selected projections. It supports terrain queries and terrain evaluation using spatial data. A common mapping toolkit is planned for TEM.
- Operations Plan/Operations Order Module—Automates the five-paragraph main body and the battlefield functional area (BFA) annexes. Key features include the ability to build the scheme of maneuver graphically and, if necessary, automatically translate it to text.
- Movement Control Module—Automates convoy planning to include management of transportation assets, creation of configurations, routing and scheduling of movement, and in-transit visibility.
- Briefing System Generator Module—Automates creation, modification, display, and presentation of tactical briefings, including maps, unit and graphic symbols, and provides a linkage to system databases.

The standards for the ACOE are summarized in Table 75.

ATCCS Common Hardware and Software for the ACOE. Supporting ATCCS are three types of communications systems. The first is single-channel combat net radio (CNR). The Army has fielded VHF/FM radios such as the AN/PRC-77 and AN/VRC-12 family of radios and is deploying the Single-Channel Ground-Air Radio System (SINCGARS). The second type is an area switched telephone system called the Mobile Subscriber Equipment (MSE) that also has mobile subscriber capabilities. A packet-switched data communications overlay for MSE is currently being added for data communications. The third type of communications, used exclusively for data transmission, is called the Army Data Distribution System (ADDS) and consists of the Enhanced Position Location Reporting System (EPLRS) and the Joint Tactical Information Distribution System (JTIDS). The data rate for EPLRS will be 2,400-3,600 bits/sec.

In addition various types of local area networks are provided for local-command-post and intra-system communications. [Ref. Levine 1994a]

Table 75. ACOE Open Systems Environment Standards Summary

Service Area	Service	Standard
Operating System Services	Kernel	POSIX.1 (FIPS 151-1)
	Command and utilities	POSIX.2 (IEEE P1003.2 Draft 11.3)
	System management	GNMP (FIPS 129, planned)
	Security	POSIX.6 (IEEE P1003.6 Draft 12)
Programming System	Programming languages and bindings	Ada (FIPS 119), C (FIPS 160), COBOL (FIPS 021-3), FORTRAN (FIPS 069-1), Pascal (FIPS 109)
	CASE tools and environment	ISEE-PCTE (planned), ISEE-SCCS (planned)
User Interface	Data stream encoding	X-Window System (FIPS 158)
	Data stream interface	X-Window System (FIPS 158)
	Subordinate foundation	X-Window System (FIPS 158)
	Toolkit components	IEEE 1201.X (future)
	Presentation	IEEE 1201.X (future)
	Dialog	IEEE 1201.X (future)
Data Management Services	Data dictionary-directory	IRDS (FIPS 156)
	Data management	SQL (FIPS 127-1)
	Distributed data	RDA (planned)
Data Interchange Services	Document interchange	ODA/ODIF (ISO 8613:1989), SGML (FIPS 152)
	Graphics data	CGM (FIPS 128)
	Product exchange interchange	IGES (planned), STEP (DIS 10303)
	Electronic data interchange	FIPS 161
Graphics Services	Graphics	GKS (FIPS 120-1), PHIGS (FIPS 153)
Network Services	Data communications	GOSIP (FIPS 146-1)
	Transparent file access	TFA (IEEE P1003.8 Draft 6)
	Distributed computing	OSF/1 NCS RPC (planned)

Source: [Levine 1994b].

The Common Hardware and Software (CHS) Program has selected an initial set of components for the COE based on the needs of the ATCCS program. The ATCCS implementation of the ACOE is shown in Figure 42. Layer 1 is the CHS common hardware. The ATCCS computers—the Portable Computer Unit (PCU) and the Transportable Computer Unit (TCU)—are based on a 32-bit Motorola 68020 microprocessor,[143] a 32-bit, 5 Mbit/s data bus, a 3.5-in floppy disk drive, and a 40- or 100-Mbyte removable hard disk cartridge. The PCU supports 1-2 million instructions per second (MIPS) and 4-20 Mbytes of random access memory (RAM), whereas the TCU supports 2-4 MIPS with 4-16 Mbytes of RAM. The Standalone Display Unit (SDU) is a 16-in monitor with two[144] configurations: monochrome display with a direct (RS-232) connection to a PCU or TCU or color monitor device (CMD) with keyboard and connection to the standard (ISO 8802.3) local area network (LAN). The PCU has a 25-line (9-in) built-in display. The stand-alone Hard Disk Unit (HDU) is a 152-Mbyte disk drive with an Institute of Electrical and Electronics Engineers (IEEE) 488 interface. The Adaptive Programmable Interface Unit (APIU) provides four modems with multiple interface options (e.g., wire, RS-232, RS-449, COMSEC,

---

143 A 68030 microprocessor is optional, supporting up to 8 MIPS (at a 33 MHz clock rate).

144 Other options include 16- or 19-in high-resolution color monitor with eight planes (the standard is six planes). A 12-in, four-plane option is also available.

combat net radio, packet switching). The Handheld Terminal Unit (HTU), designed as a digital entry device for forward units, weighs 7-10 lb and supports up to four modems.

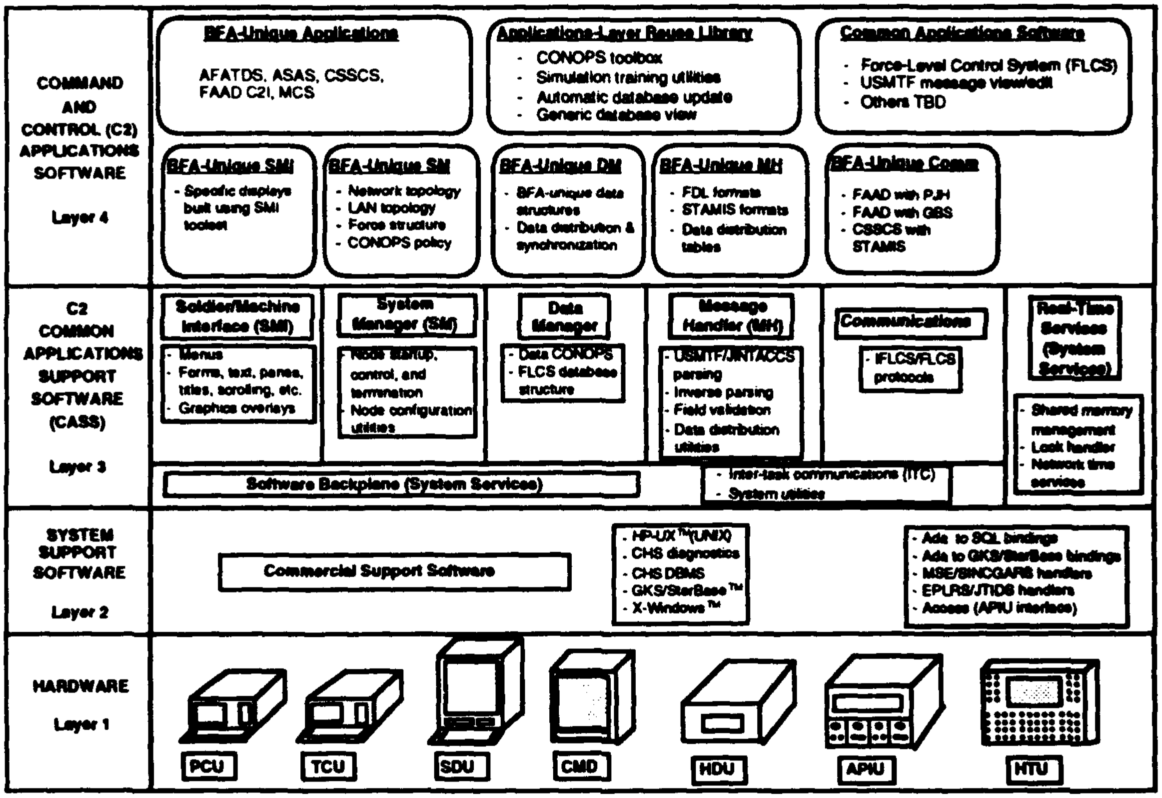
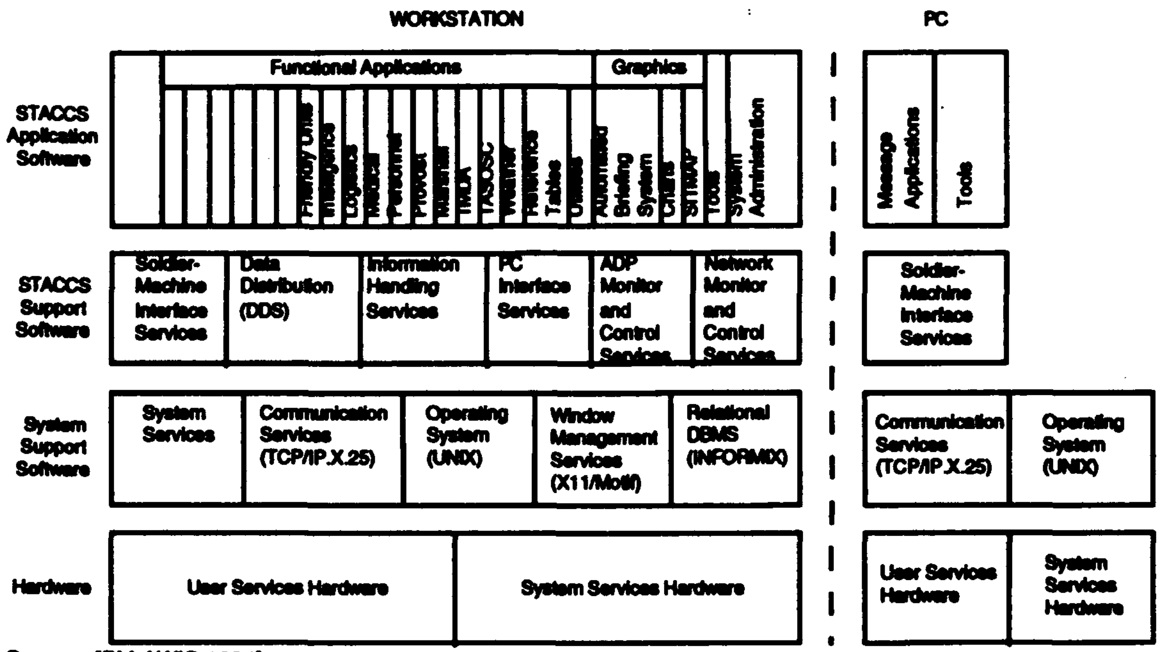


Figure 42. Current Implementation of ACOE for ATCCS with CHS

The ATCCS CHS Layer 2 software is provided with the NDI hardware and includes both UNIX and MS DOS environments (the HTU supports only MS DOS). Layer 2 has an Ada environment with programming support tools and standard tools accessible via bindings in Ada for graphics [e.g., Graphics Kernel System (GKS) and database management (e.g., Starbase and SQL query interfaces)]. Layer 2 also provides handlers and access codes for the communications hardware and software (e.g., APIU, LAN). Protocols for ATCCS are summarized in Appendix C.

Army Global Command and Control Systems (AGCCS). The Army component of the Joint Global Command and Control System (GCCS) is the AGCCS. The AGCCS will be built from applications programs developed by the Army WWMCCS Information System (AWIS), the Standard Theater Army Command and Control System (STACCS) (which in turn evolved from UTACCS and AC2IS), and the Echelon Above Corps (EAC) portion of the Combat Service Support Control System (CSSCS). The request for proposal (RFP) to migrate these three systems into AGCCS is currently in preparation with contract award planned for 1Q FY95. The primary scope of this effort will be to evolve these stand-alone systems into a suite of modular applications (such as logistics, medical, personnel, Theater Army Special Operations Support, Mobilization and Development, Army Status of Readiness and Training, Transportation Asset Management, etc.) that execute on the ACOE, and interface with common applications and other shared components of the ABCS. Descriptions of the three AGCCS components are as follows [Ref. Levine 1994b]:

- AWIS fulfills the Army's strategic C2 requirement for software, hardware, and databases for the implementation of the Joint Operations Planning and Execution System (JOPES) and other joint service systems that support the Commanders-In-Chief (CINCs) and Joint Chiefs of Staff (JCS). In addition, AWIS modernizes the Army's C2 system supporting conventional military planning and execution.
- STACCS is a peacetime and go-to-war system, primarily aimed at assisting a theater commander in the execution of crisis and wartime EAC sustainment and operational maneuver functions. STACCS also interoperates with the Global Command and Control System (GCCS), sister services, multinational and ATCCS Battlefield Functional Area Control Systems (BFACS)/ABCS, and other command and control systems. The current implementation of the ACOE for STACCS is shown in Figure 43.
- CSSCS (EAC) will consolidate and collate the vast quantities of data required to integrate situational awareness of the combat service support mission areas. CSSCS will provide strategic and tactical commanders with timely, critical information on ammunition and fuel supplies, medical and personnel status, transportation, maintenance services, general supply, and other field services.



Source: [PM AWIS 1994].

Figure 43. Current Implementation of ACOE for STACCS

Army Battle Command System (ABCS). The ABCS requirement is for a standard modular system and application software supporting a "tailorable" suite of functional applications residing on the ACOE and common hardware platforms in order to meet a specific set of commander's information needs in the execution of a specific mission or task. ABCS will link strategic, theater, Joint, and allied C2 systems across the full range of battlefield and operations other than war functions. The ABCS is the emerging Army concept for the Army "system of systems" utilizing a seamless architecture evolving from the ATCCS from echelons above corps (EAC) through brigade and below. [Ref. Levine 1994b]

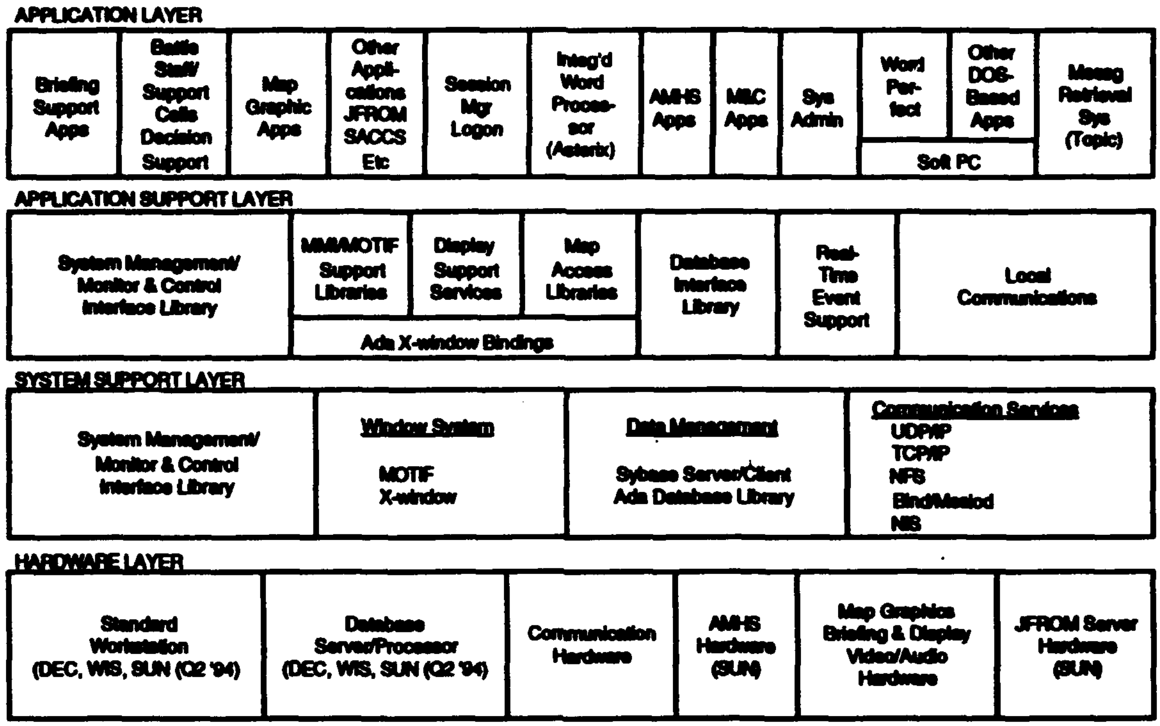
ABCS Migration Strategy. The ABCS baseline carrier is the ACOE, which is substantially in synchronization with standard operating environments of all the other Services. The echelons corps and below (ECB) portion of ABCS is known as the ATCCS Battlefield Functional Area Control System (ATCCS BFACS), which comprises MCS, ASAS, AFATDS, FAAD C2I, and CSSCS (Corps and Below). The ATCCS BFACS will evolve from the current suite of ATCCS "systems" to interoperable applications running on the ACOE. Significant systems engineering and programmatic analysis is currently in progress by the US Army Program Executive Officer for Command and Control Systems (PEO CCS) to achieve this migration. This strategy is being developed to determine the most cost-effective cut-over points for each of the systems into an integrate ABCS, taking into consideration the current programmatic status of each system. AFATDS, ASAS, and CSSCS are currently in development and under contract. ASAS successfully completed initial operational test and evaluation (IOT&E) in 1993, while AFATDS and CSSCS will complete IOT&E in 1994. The migration process has commenced with the maneuver battlefield functional area. The Maneuver Control Block IV RFP is in the final stages of preparation, and is written in response to ABCS requirements. Initial fielding of the maneuver application of ABCS is planned in 1995, with accelerated fielding to the Army, making maximum use of previously fielded (MCS Block III) hardware. [Ref. Levine 1994b]

Integrated Meteorological System (IMETS). IMETS is a low-density single-function weather correlation and reporting system specifically designed and implemented to support the commander and soldier via full-time interoperability with ABCS and the US Air Force Global Weather Service (USAFGWS). IMETS is Army owned and operated by USAFGWS weather personnel. IMETS employs the ACOE to the maximum extent possible. IMETS employs standard Army shelters and is fully mobile and transportable. There are no plans to migrate IMETS into another system or systems.

Combat Terrain Information System (CTIS). CTIS in the US Army refers to the integration of the Digital Topographic Support System (DTSS) and the Quick Reaction Multicolor Printer (QRMP) programs. CTIS, a low-density system, employs the ACOE to the maximum extent possible. CTIS receives IMETS weather products and available enemy map data, stores this information in a database, and provides current map overlays and terrain and mobility analyses (using DMA map products) as either digital or paper-copy products. CTIS provides extremely rapid color products of the map/terrain output (e.g., in paper form). All products are available worldwide, since the CTIS capability is fielded in standard Army shelters and is C-130 capable. There are no plans to migrate CTIS into another system. [Ref. Levine 1994b]

Counter-Narcotics Command Management Control System (CN/CMS). CN/CMS is a Joint DoD/Drug Enforcement Agency (DEA)/Department of Justice (DoJ) program. The Army is the executive agent for this system; PEO CCS is the Army implementor. CN/CMS provides computer and secure voice functionality to DoD, DEA, DoJ and other special users at DoD, Department of State (DoS), and law enforcement agencies in the continental United States (CONUS) and outside the continental United States (OCONUS) in support of counter-narcotics operations. Up to 40 sites in 16 countries (to include US) are planned to be completely installed and fully operational by 30 September 1995. There are no migration plans for the CN/CMS, although the system employs the ACOE to the maximum extent possible. CN/CMS will be the target system. [Ref. Levine 1994b]

USAREUR Command Center System (UCCS). UCCS provides an integrated information, message, map, and briefing development and display capability at the CINC level. Figure 44 shows the current implementation of the ACOE for UCCS.



Hardware and System Support Layer and some Application Layer Components are COTS or GFE

Source: [PM AWIS 1994].

Figure 44. Current Implementation of ACOE for UCCS

MTACCS Architecture. The Marine Tactical Command and Control System (MTACCS) concept is shown in Figure 45. One of the tactical C2 systems is specifically assigned the role of a force-level control system to support Marine Air-Ground Task Force (MAGTF)-level C2. Central to MAGTF C2 is ADP support for a MAGTF Database developed from information provided in the four functional areas. These are Ground C2, Aviation C2, CSS C2, and Intelligence. MAGTF C2 provides support to the Commander for information fusion, dissemination, and display; planning; assessment; and tasking. The Marine Corps has developed a Common Application Support Software architecture, similar to the one illustrated in Figure 42 (above) for the Army.

The Ground C2 functional area includes maneuver control and fire support, as well as integration of position location information (PLI). Aviation C2 includes offensive and defensive air support, to include fixed-wing and rotary wing vertical takeoff and landing assault support and antiair warfare. In addition, Aviation C2 includes control of aircraft and missiles, electronic warfare, and air reconnaissance. CSS C2 provides visibility to the MAGTF and other functional areas as required on logistic assets and manpower. Intelligence supports MAGTF C2 by providing information on enemy positions, orders or battle, and maneuver indicators.

Copernicus Architecture. Tables 76 and 77 illustrate the Copernicus architecture developed by the US Navy for strategic and tactical systems. Copernicus is a "seamless"

information management architecture for Navy command, control, communications, computers, and intelligence (C4I) consisting of four pillars: eight Global Information Exchange Systems (GLOBIXSs), the Command-in-Chief (CINC) Command Center or Complex, four Tactical Data Exchange Information Systems (TADIXSs), and the Tactical Command Center.

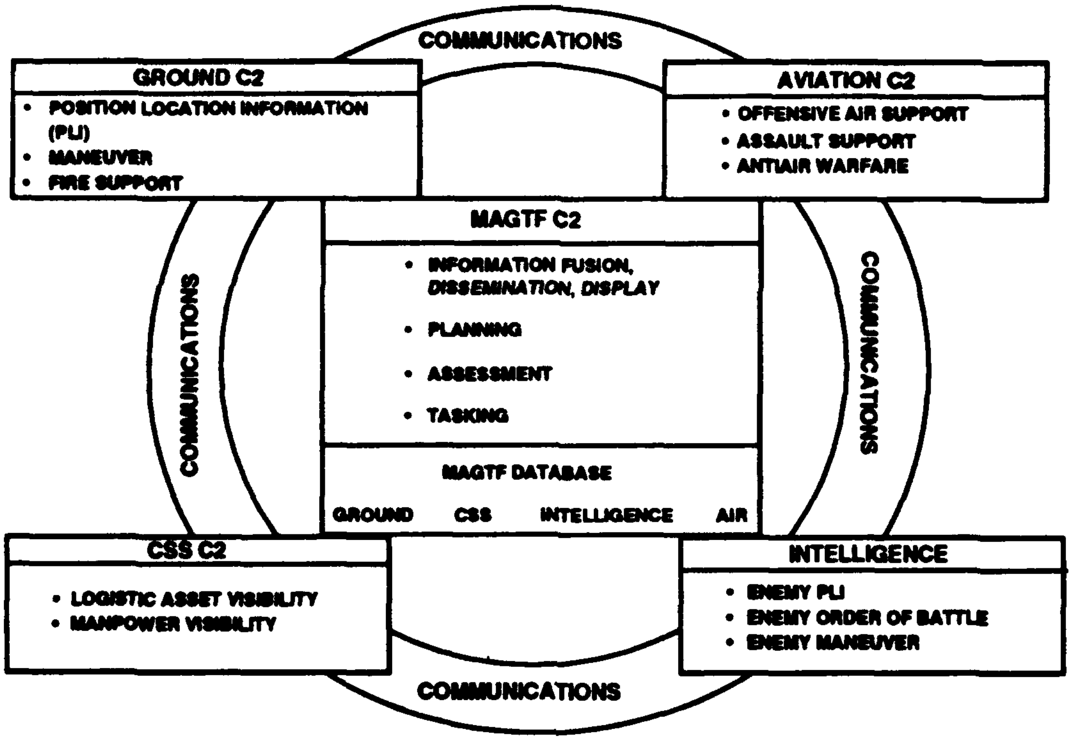


Figure 45. US Marine Tactical Command and Control System (MTACCS)

Copernicus capabilities will be implemented in a building block approach. Each GLOBIXS will be a global, virtual (not necessarily physically dedicated) network of the Defense Communications System (DCS). Each GLOBIXS will be an afloat virtual network of variable duration (minutes, hours, or days), depending on the information exchange load. The CINC Command Complex consists of workstations; local area networks; the Base Information Transfer System (BITS—a wideband, local, and metropolitan area network) with network management, security, standards, and protocols; database; and communications servers. The Tactical Command Center has similar capabilities using the newly developed Communications Support System (CSS) instead of BITS.

The Copernicus architecture for the information systems (CINC Command Complex and Tactical Command Center), specifically to address interoperability, has three parts: (1) standards and protocols, (2) security, and (3) network management. As with ATCCIS, the US Navy has determined that homogeneity is not practical and that "users need open systems that provide interoperability of products and portability of people, data, and applications across heterogeneous computing environments." The standards will include POSIX and GOSIP, but these have been determined as "not sufficient to address the full spectrum of needs, even in their range of applications." As a result, the Navy has adopted the APP/OSE developed by NIST to facilitate rapid prototyping, evolutionary acquisition, implementing various computer architectures, refocusing research and development, leveraging research and investment, and achieving the goal

of scaleability of hardware and software capabilities and standards that will be required in the future. [Ref. COPERNICUS 1991]

Table 76. US Navy Copernicus Architecture—Pillars, IERs, and Functions

Information Management Ashore		Information Management Afloat	
GLOBIXSs A. SIGINT Mgmt B. ASW Mgmt C. SEW Mgmt D. HICOM E. Imagery Mgmt F. Database Mgmt G. RDT&E Coord H. Navy-Wide Administration	**CINC COMMAND COMPLEX** 1. Unified Commands 2. Other Services 3. Navy • FOSIC • FIC • CSG • ASW • SEW • Watch • Research • C2 Center	**TADIXSs** A. Command B. Support C. Direct Targeting D. Force Operations	**TACTICAL COMMAND CENTER** 1. Composite Warfare Coordinator 2. Antiair Warfare Center 3. Anti-Submarine Warfare Center 4. Anti-Surface Warfare Center 5. Space & Electronic Warfare Center 6. STWC
Information Exchange Requirements • Voice • File Transfer • Imagery • Interactive • Messages • Real-Time Data • Video	• Receive & process info • Maintain C2, intelligence, strategic & tactical info • Generate command displays • Support query & response • Provide models & other C2 decision aids • Generate & monitor orders, plans, & related information • Support operator training • Provide system monitoring & control	Information Exchange Requirements • Voice • File Transfer • Imagery • Interactive • Messages • Real-Time Data • Video	• Receive & process info • Maintain C2, intelligence, & tactical information • Generate cmd displays • Support query & response • Provide models & other C2 decision aids • Generate & monitor orders, plans, & related information • Afloat adaptability • Shipboard training support • Provide system monitoring & control

Sources: [OP-094 1991]; [Ornstein 1991].

For security, Copernicus will use the capabilities development for the DoD ICA, including both end-to-end and multi-level security devices. For network management, Copernicus will use MIL-STD-1813, *Network Management for DoD Communications*, June 1991, developed by NIST.

Navy and Air Force Common Operating Environment. The Departments of the Navy and Air Force had extended discussions in 1993 to explore the agreement and future development of a COE for the C2 systems of the Air Force, Marine Corps, and Navy. Elements of this COE are based on both the Navy's Unified Build for the Joint Maritime Command and Information System (JMCIS) and the Air Force's Contingency Tactical Air Control System (TACS) Automated Planning System (CTAPS). A paper describing these recommendations is planned for early 1994.

Air Force Computer-Communications Architecture. The architecture currently addresses base-level applications that are stove-piped and are hosted on a standard base-level computer, but these concepts are evolving to a local information transfer environment with support from regional processing centers. An Air Force Corporate Data Dictionary is being developed. The Air Force software architecture is illustrated in Table 78.

Table 77. US Navy Copernicus Architecture—Functional Architecture

Model	Component of Architecture	Planned Building Block
Open Systems Architecture	Common Human-Machine Interface	
Common Message and Data Transmission Formats	Software Applications and Utilities	• Data compression software • Sensor-specific data • Cross-correlation data • Data robots • Copernicus tactical software • Common decision support software • Environmental analysis software • Trans-sanitization software • INFOSEC (COMPUSEC, COMSEC) software • Network and system management software
	Application Portability Interface (POSIX Standard)	
	Operating Systems	• COTS operating systems (e.g., UNIX, VMS, DOS)
Open Systems Standards and Communications Protocols (GOSIP) Standard BUS architecture and Hardware Interfaces	Hardware	• Desktop engines (e.g., personal computers) • Workstation engines (e.g., DTC-2, TAC-3) • Communications servers • Data File servers • Display devices • Modular embedded cryptographic devices • STU III COMSEC devices • Interchangeable modems • Standard storage devices
Nondevelopmental Items (NDI) (Commercial off the shelf and government off the shelf)	Network Services from Common User Backbones	• GLOBIXSs (using DDN, DSN, DCTN, TelCo, etc.) • TADIXSs (using CSS: SATCOMs, HF, LOS, etc.) • LANs (e.g., (IC)2, SAFENET, etc.)

Source: *The Copernicus Architecture*, Briefing to IDA, Space and Electronic Warfare Directorate OP-094 (CAPT J.R. Wood), October 1991, UNCLASSIFIED.

Table 78. US Air Force Software Architecture

<table>
<tr><td colspan="3"><u>User Interface</u>
X-Windows</td><td rowspan="4">GOSIP</td></tr>
<tr><td colspan="3"><u>Applications</u></td></tr>
<tr><td>Commercial <u>Off-the-Shelf</u>
Word Processors
Graphics</td><td><u>Tools</u>
CASE
Data Dictionary</td><td><u>Developed</u>
Ada
SQL
Data Standards</td></tr>
<tr><td colspan="3">POSIX

<u>Hardware</u>
Micro-computer   Mini-computer   Mainframe   Supercomputer</td></tr>
</table>

Source: *Air Force C4 Architecture*, Briefing to JTC3A's Objective Architecture Conference, HQ USAF/SCX (LTC J.M. O'Meally), September 1991, UNCLASSIFIED.

CTAPS Common Operating Environment. CTAPS was developed during the period 1986-1991 based on a comprehensive software standards-based environment. These standards were adopted in 1991 by the General Officer Steering Committee as the Tactical Battle Management (TBM) standards. They comprise the following [Ref. Pait 1994]:

- Operating system: POSIX-compliant version of UNIX
- Communications/networking: TCP/IP over ISO 8802-3 (Ethernet), with future transition to GOSIP standards
- User interface: OSF/Motif and X-Windows
- Data management: ANSI SQL-based relational database management systems (Oracle and Sybase)
- Data manipulation and query: ANSI SQL
- Graphics: GKS for two-dimensional graphics with transition to PHIGS for three-dimensional applications, when available
- Mapping: Air Force's Common Mapping Program.

Because of early use of standards-based products (UNIX and Oracle) and the subsequent evolution of the standards and because product-unique extensions were used by implementors, elements of CTAPS implementation are not compliant with the newest versions of POSIX and SQL. This is planned to be addressed as block changes are made in CTAPS.

The Air Force is looking at the broad issues associated with choosing standards and standards-based products and simultaneously planning the evolution towards increased openness in the underlying architectures. The approach is to carry the standards-based approach used in CTAPS further through the use of open systems standard applications interfaces (OSSAIs). These OSSAIs range from style guides to specific POSIX interfaces to applications. Each OSSAI standardizes dialogues, not the functionality of applications or other processes. OSSAIs would be provided between applications and users, operating system, databases, and other applications. The standards being consider for these OSSAIs are based on the POSIX OSE Reference Model (P1003.0) and includes the following [Ref. Pait 1994]:

- POSIX and POSIX application program interfaces (APIs) defined by ISO 9945, FIPS 151-1, ISO JTC1 SC22/WG15, and IEEE P1003 projects
- GKS (ISO 7942:1985), GKS-3D (ISO 8805:1988), PHIGS (ISO 9592), PHIGS Plus, and the PHIGS Extensions to X-Windows (PEX)
- X-Windows, Xt Intrinsics, Xlib, and FIPS 158
- OSF/Motif and OPEN LOOK graphical user interfaces
- Reference Model on Data Management
- SQL (ISO 9075; ANSI X3.135), Embedded SQL (ANSI X3.168), and evolving extensions to SQL (SQL2 is now part of ISO 9075; SQL3 is under development)
- RDA and the SQL specialization of RDA
- IRDS (ANSI X3.138-1988)
- TCP/IP and OSI interconnection standards, to include X.400 MHS, X.500 Directory, FTAM (ISO 8571), RPC, X.25, ISO 8802-3 (IEEE 802.3) Ethernet LAN, ISO 8802-5 (IEEE 802.5) Token Ring LAN, and FDDI.

Coast Guard Information Systems Architecture. The Coast Guard has a diversity of requirements stemming from the need to communicate and interoperate with many government agencies. The Coast Guard has developed a standards-based architecture with eight aspects: network standards, hierarchical structure, decision support systems, sensor sub-architecture,

information security, public data interface, radio navigation mapping, and command center mapping.

US Army Initiatives. The US Army has a number of initiatives underway that address tactical implementations of OSI standards. The initiatives are under the direction of the Interoperability and Standards Directorate of the Communications-Electronics Command. The Army has an initiative to evaluate OSI protocols (including possible enhancements) in the newly developed Single-Channel Ground/Air Radio System (SINCGARS) combat net radio (VHF-FM). Specifically, the Army is examining options to provide an automatic voice/data contention resolution protocol at the Medium Access Control (MAC) sublayer of the data link layer (Layer 2). Some investigation of a forward error correcting Layer 2 protocol is also ongoing. In addition, an OSI profile is being developed for a local area network (T.LAN). Further, the Army has procured with its Common Hardware and Software (ATCCS CHS) nondevelopmental item (NDI) program a number of commercial OSI implementations, including ISO 8802.2 and 8802.3 for the local area network (TCP/IP and other DoD protocols will be used initially at layers above Layer 2). CHS has ITU-TS X.25 switched protocols for wide area networks (these also are used in conjunction with TCP/IP). Finally, the CHS has a standard graphics interface and plans in the next procurement phase to obtain, if possible, a POSIX-conformant operating system. [Ref. CECOM 1989]

US Marine Corps Initiatives. The Marine Corps has adopted a Technical Interface Design Plan (TIDP) for Marine Tactical Systems (MTS) [Ref. MTS TIDP 1987] that mandates the use of bit-oriented messages and two functional profiles for protocols in all its command and control systems. One profile for broadcast mode is designed to be used in combat net radio. It has been implemented in the AN/PSC-2 Digital Communications Terminal (DCT). The second profile of protocols is for switched mode and was developed from the Joint Tactical Communications Program (TRI-TAC) Interface Control Documents. This profile has been implemented with the Unit Level Tactical Data Switch (ULTDS). The switched profile is also being implemented with the Tactical Air Operations Module (TAOM) and a developmental system for air operations—Advanced Tactical Command and Control Center (ATACC). Although not fully OSI conformant, the two MTS profiles are based on several OSI standards (ISO 3309, ISO 7809, and ISO 4335). The Marine Corps' approach to data communications standards and profiles follows the OSI seven-layer model and incorporates military features not covered within the ISO standards.

Army and Marine Corps Initiatives in Fire Support. The Army and Marine Corps are cooperatively building an Advanced Field Artillery Tactical Data System (AFATDS), which is going through initial operational test and evaluation and which has a major Army decision milestone at the end of 1994. AFATDS will replace the Tactical Fire Direction System (TACFIRE) in the Army, which is currently in Version 10 (V.10). Both Services have fielded an interim system for fire support for battalion fire direction centers. In the Army, this system is known as the Lightweight TACFIRE, since it has the capability of Battalion TACFIRE in a portable, military-specification workstation. In the Marine Corps, this system is known as Marine Corps Fire Support System (MCFSS). Both run software compatible with V.10 TACFIRE, including TACFIRE messages and protocols (similar, but not identical, to the messages and protocols of STANAG 4202 and STANAG 5620). Both systems use RS-232C physical interfaces and ISO 8802-3 (IEEE 802.3) with TCP/IP for local area networks interconnecting these devices. Both Services use combat net radio (CNR) to exchange digital data (and voice)—the Marine Corps uses VRC-12 and PRC-77 radios, while the Army uses these together with SINCGARS. Eventually the two systems will be identical and known (in the Army, at least) as the Interim Fire Support

Automation System (IFSAS). Eventually, it is intended to implement the MIL-STD-188-220 and Variable Message Format (VMF) (see Appendix C) interfaces. Study is also being made of interface to tactical packet switches, whose protocols are described in Appendix C. [Ref. PNL 1994]

19.11.8 DoD Internet Protocols

DoD Protocol Suite. Figure 46 shows the DoD Internet protocol suite.[145] The upper layer protocols providing user functionality support file transfer [File Transfer Protocol (FTP),[146] MIL-STD-1780]; electronic mail [Simple Mail Transfer Protocol (SMTP), MIL-STD-1781]; and remote system access [TELNET Protocol,[147] MIL-STD-1782]. The middle layers provide a reliable host-to-host transport protocol [Transmission Control Protocol (TCP) MIL-STD-1778] on top of a connectionless (CL) internetworking protocol.

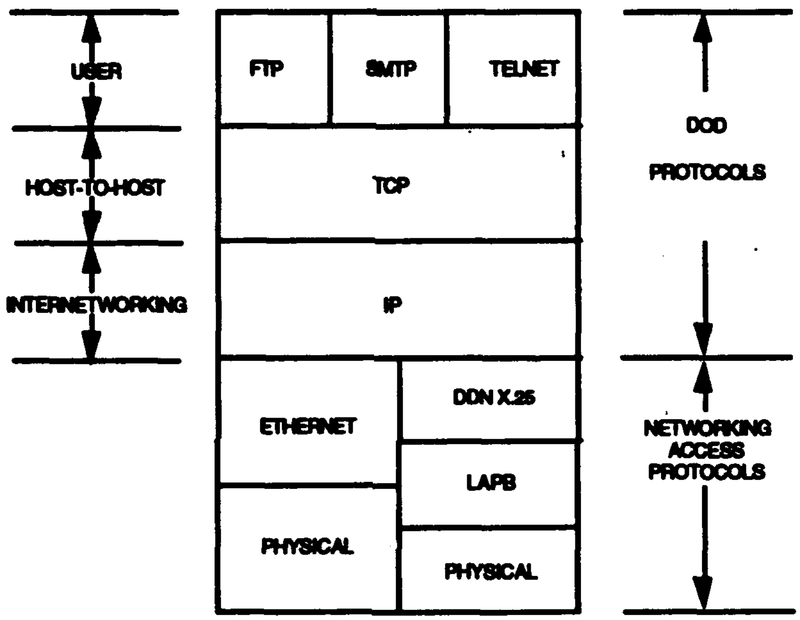


Figure 46. DoD Protocol Suite

No lower layer protocols are specified in the DoD protocol suite—it uses whatever protocols are required to access the network to which it is attached. Thus, for example, the DoD protocol suite uses the Ethernet™ (ISO 8802.3 CSMA/CD Media Access Control for a coaxial cable 10-Mbps LAN) protocol to operate of a local area network and the DDN implementation[148] of the ITU-TS X.25 protocol (X.25 Packet Level Protocol, ISO 8208) and the HDLC LAPB (ISO 7776) procedures to operate over a wide area packet switching network. Although DoD

145 The figures and information for this section and the following sections on US GOSIP and proposed mixed stacks for Army CCISs is taken from "Use of OSI Protocols for US Army Tactical Command and Control Applications," Richard Nieporent and Brajesh Mishra, The MITRE Corporation, *Proceedings of the SHAPE Technical Centre Military OSI Symposium*, 6-8 June 1990, NATO UNCLASSIFIED.

146 FTP provides a simple application for transfer of ASCII, EBCDIC, and binary files.

147 TELNET Protocol provides a simple scroll-mode terminal capability.

148 The DDN implementation of X.25 was provided by Bolt Beranek and Newman. It is also planned for use in the Mobile Subscriber Element (MSE) for Army area communications.

protocols are not international standards, they have become a de facto open standard in the US—almost every vendor provides the DoD protocols in their version of the UNIX operating system. The DoD protocols are also included in the ATCCS Common Hardware and Software (CHS) procurement and are specified for use over the CHS IEEE 802.3 (ISO 8802.3) tactical LAN. Finally, the DoD protocols are used by the MSE packet switched network (PSN).

The DoD protocol suite has two drawbacks for their use in tactical CCISs:

- They are not US GOSIP compliant. It would be necessary for implementations of the DoD Protocols to undergo an expensive and time-consuming transition to satisfy the GOSIP mandate. In particular, the battlefield functional area (BFA) applications will have to be modified to use the functionality of the GOSIP protocols.
- GOSIP Application Layer protocols provide more functionality than the DoD protocols. Moreover, more effort is now being committed by the nations for the OSI protocols than by the US in the DoD arena. As new OSI protocols are developed that meet tactical communication requirements, they are expected to be incorporated in GOSIP. Thus, future versions of GOSIP are expected to provide considerably more functionality than the DoD protocol suite.

Version 2 of US GOSIP. Figure 47 summarizes the US GOSIP protocol suite for Version 2 (see Section 16.1.3 for the complete diagram). The applications supported are the same as the DoD protocols: file transfer (FTAM, ISO 8571), electronic mail (MHS, ITU-TS X.400-series 1984 recommendations;[149] and MOTIS, ISO 10021 and 9066], and the Virtual Terminal Protocol (VTP, ISO 9040 and 9041). Also, like the DoD protocol suite, a transport protocol (Transport Class 4, ISO 8073) is specified that will provide reliable host-to-host communications, and a CL network protocol (CLNP, ISO 8473) is specified for internetworking. Unlike the DoD protocols, US GOSIP provides for the Layer 7 Association Control Service Element (ACSE, ISO 8650), connection-oriented protocols for the Presentation Layer (ISO 8823, Layer 6), and connection-oriented protocols for the Session Layer (ISO 8327, Layer 5).

However, unlike the DoD protocol suite, GOSIP explicitly specifies a number of network access protocols, including IEEE 802 (Logical Link Control, ISO 8802.2; CSMA/CD, ISO 8802.3; Token Bus, ISO 8802.4; and Token Ring, ISO 8802.5) for communications over a LAN and the X.25 protocol for wide area packet switch network communications.

There is one major disadvantage to using GOSIP in Army CCISs now. The MSE PSN internetworking capability for tactical area communications can not be used with GOSIP, since GOSIP has a different internetworking protocol (CLNP) than the DoD protocol suite (IP). Access to the MSE PSN will still be possible using a direct interface to the tactical LAN.

Mixed Protocol Stacks for Future Army CCISs. The US Army is developing an automated Army Tactical Command and Control System (ATCCS) for the tactical battlefield. Communications connectivity for the ATCCS will be provided by the US Army's local and wide area tactical communications networks. A protocol suite must be selected for the ATCCS that can interface to these tactical networks and support a wide range of tactical communications applications. A mixed protocol suite, consisting of OSI upper layer protocols operating with the US DoD transport and internetworking protocols (TCP/IP), has been recommended to support the

149 US GOSIP 1.0 and 2.0 mandate use of X.400(MHS)-1984. US GOSIP 3.0 is expected to require X.400(MHS)-1988.

required ATCCS functionality and interoperability and provide a direct migration path to US GOSIP and the NATO militarized OSI protocols.

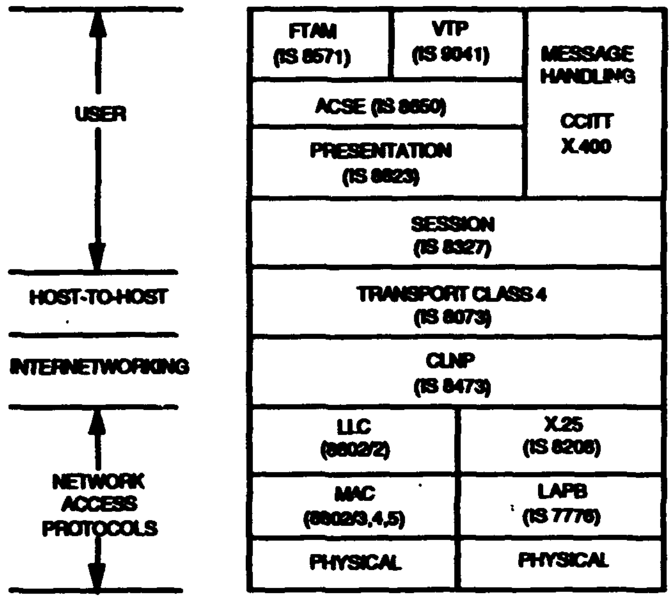


Figure 47. US GOSIP Protocol Suite, Version 2

Figure 48 shows a proposed mixed suite of protocols for ATCCS. The upper three layers consists of the GOSIP Session, Presentation, and Application Layers. The same FTAM, X.400, and VTP Application Layer protocols are specified as in GOSIP. The middle protocol layers are the same as in the DoD protocol suite: TCP and IP. Also, as in the DoD protocol suite, the lower layer protocols (Physical, Data Link, and Network Layers) are unspecified.

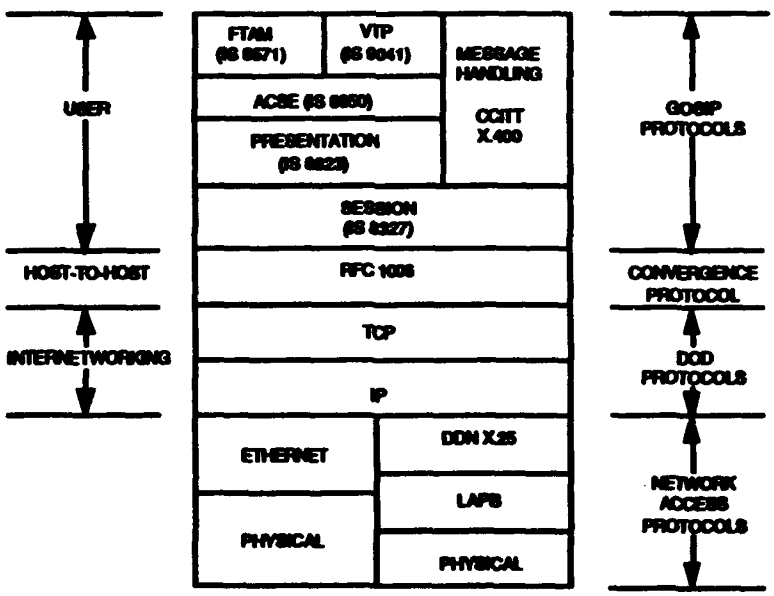


Figure 48. Proposed Mixed Protocol Suite

The mixed protocol suite has the increased functionality of the GOSIP Application Layer protocols, without sacrificing compatibility with the MSE PSN. No changes will be necessary in BFA applications, when ATCCS transitions to GOSIP, since they would already use the GOSIP Application Layer protocols. [Ref. Nieporent 1990]

A Convergence Protocol [Request for Comment (RFC) 1006, *ISO Transport Service on Top of the TCP*, Version 3, 1987] is needed to interface the GOSIP upper layer protocols to the DoD internetworking protocols. The Convergence Protocol provides OSI Transport Class 0 (TP0) along with a packetization protocol.[150] This protocol is commercially available in Version 6.0 of the ISO Development Environment (ISODE).

19.12 Identification of Efforts to Evaluate the Performance of Civil Standards for Military Use

This section identifies a number of papers submitted in June 1990 to the Military OSI Symposium at SHAPE Technical Centre that describes analytical and demonstration efforts to evaluate the performance of OSI and other protocols for use in military systems. These papers should be consulted for detailed results.

19.12.1 Tactical Communications Requirements and OSI Applications[151]

The issue of whether or not tactical message delivery requirements can be met by the deployment of OSI applications in the tactical environment does not have a simple answer. A recent study conducted on behalf of the US Army examined the various attributes of FTAM and X.400 from the perspective of tactical communication systems and requirements. Both FTAM and X.400 provide highly reliable, in-sequence data delivery, but they provide no guarantees about the delivery delay. It was concluded that if delivery delay, rather than reliability, is the dominant requirement for a specific application, then consideration should be given to the use of connectionless application-layer services, which is allowed by GOSIP.

It was also concluded that since real-world applications are seldom monolithic, it is unlikely that all of the requirements of a specific application can be met by a single GOSIP application, such as FTAM or X.400. Considering the broad range of message length and delivery delay requirements of most tactical applications, it is likely that both high-performance messaging and data transfer capabilities will be required in most environments. In addition, deployment of some form of connectionless application-layer protocol appears necessary to meet near-real-time application needs, where near-real time is defined as highly reliable delivery within about 1 minute.

Tactical Communications and OSI Protocols. The study found that some of the tactical radio systems, such as MSE and SINCGARS (with appropriate host processing add-ons) have sufficient bandwidth and processing power to support deployment of OSI protocols. On the other hand, given the requirements of the tactical applications, OSI applications such as X.400 and FTAM require substantial networking resources to support their requirements. Considering the strict delivery requirements of some of the tactical applications, it appears that standard OSI applications would not always provide the high performance messaging and/or data transfer that would be needed in the tactical environment. Standard, streamlined, high performance protocols

---

150 Since TCP is a stream-oriented protocol and TP0 is a block-oriented protocol, the packetization protocol is needed to preserve the OSI packet boundaries.

151 Based on *Thin Stacks for Military Tactical Radio Applications*, September 1993 [MITRE 1993].

and applications could be developed for use throughout the tactical environment and interoperated with standard OSI applications through application gateways.

Communication Protocol Alternatives. Since tactical systems have limited processing and transmission resources, three methods of reducing the demand placed on these resources by OSI protocols were considered: functional thinning, layer reduction, and header encoding.

In the functional thinning, or "thin-stack" approach, the idea is to reduce transmission and processing requirements by carefully examining the functions provided by each of the upper layers in the protocol stack and eliminating those that are unnecessary. It was determined that creation of a "thin stack" provides no benefits with regard to reducing the required protocol transmission bandwidth. Although such modifications may require little new software development, the resulting "thin stacks" will not be commercial or government off-the-shelf (COTS/GOTS), and therefore, many of the benefits of deploying GOSIP in the tactical environment would be negated.

The idea in the layer reduction approach is to combine upper layer protocols into a smaller number of layers in order to reduce processing and transmission needed to coordinate the activities of the various layers. This reduction seems to provide benefits related to reducing the processing bandwidth required for supporting the OSI protocols, but the reduction in the transmission bandwidth overhead achieved may not be significant. Furthermore, such radical alterations of the OSI protocol stack would introduce interoperability problems with full OSI stack implementations.

In the header compression approach, the idea is to simply compress the headers required by each of the layers in order to reduce the number of bits that must be transmitted between systems. Header compression via bit mapping appears to be infeasible because it adds to the processing load and also creates a strategic/tactical interoperability problem. Header reduction via the packed encoding rules (PER) appears to be a good option in that it represents a one-for-one replacement of the basic encoding rules (BER), which is already a requirement of GOSIP.

Summary of Results and Recommendations. OSI was not recommended for use in combat net radio (CNR) or comparable tactical radio systems that must support near-real-time delivery requirements. For more bandwidth and processing-capable radio systems (e.g., MSE and SINCGARS with appropriate host processing add-ons), a full OSI stack can be deployed to service traffic having less demanding delivery requirements. In order to reduce the costs of developing a new OSI profile, the study recommended that the DMS OSI profile developed for the strategic environment be considered for those tactical environments capable of supporting the full OSI stack.

For CNR-like tactical radio systems, it does not appear that any level of OSI protocol functional thinning would result in a protocol suite that would be capable of supporting the strictest message delivery requirements of the tactical environment. Development of a tactical application protocol (TAP) designed specifically for the highly mobile/near-real-time messaging supported by the CNR systems should be considered. The development of this protocol could be tied into the ongoing work on the Digital Message Transfer Device (DMTD). Effort should be made to ensure that any protocols developed for the tactical environment will support mobile routing requirements needed to support internetworking for tactical communication systems.

OSI can, however, be used within the tactical switched systems to support the less time-critical message transmission requirements. X.400 has a clear application use in the tactical

switched environment: message interoperability with DMS, relatively time insensitive messaging, imagery dissemination, and interconnection of dissimilar systems - an X.400 messaging backbone.

Interoperability between those tactical systems deploying TAP and those tactical and strategic systems deploying DMS-OSI could be restored through the deployment of dual protocol stacks in some (or all) of the switched radio systems. It should be noted that this approach toward interoperability is necessary regardless of what non-GOSIP protocol stack is adopted by the tactical radio environment.

Since the communication infrastructure requirements to support deployment of FTAM are essentially the same as those required for the deployment of X.400, FTAM can be deployed in any environment where X.400 can be deployed. The usefulness in a specific application would depend upon the needs of that application. For example, if fetching a file from a remote system is a requirement of a particular application, then FTAM would provide the required functionality.

It is recommended that test deployments of X.400 be made with candidate tactical radio systems. Prime candidates, due to the applicability of their architecture and mission, are MSE and SINCGARS. As it is possible to implement X.400 over either OSI or DoD lower-layer protocols, it is recommended that initial testing be performed over a Transmission Control Protocol/Internet Protocol (TCP/IP) based subnetwork. This would allow for a more rapid, and less risky, initial deployment. Following success of the initial tests, experimental tests of X.400 over pure OSI protocol stacks should be considered. In order to quickly test the feasibility of using X.400 in systems such as MSE or SINCGARS, it is recommended that initial tests use standard COTS implementations.

19.12.2 Additional Analyses

Practical Evaluation of OSI Protocols. This paper summarizes work being done under the Robust Protocols Research Programme at the Defence Research Agency in the UK MOD. The work has concentrated on X.400 and FTAM over TP4, CLNS, and X.25. [Ref. Price 1990]

User Performance of Tactical Networks in the ITDN. User performance experiments were conducted in 1989 on portions of the Integrated Tactical-Strategic Data Network (ITDN) Demonstration that simulated tactical areas at echelons corps and below. The performance of four tactical links [Fleet Satellite Communications (FLTSATCOM), MSE line-of-sight radio, Tactical Satellite Communications (TACSATCOM), and Very Small Aperture Terminal (VSAT)] was measured at the protocol level that most directly affects the network user. The results, though preliminary, can help predict the performance of applications in tactical nets. US DoD protocols were measured; however, the results may provide the basis for informed conjectures about the user-level performance of OSI protocols. [Ref. Reichlen 1990]

Transport Protocols and Internetworking in Low Bandwidth Tactical Networks. This paper examines the impact of packet size on end-to-end functionality (including reliable delivery, packet resequencing, segmentation, and flow control). Tradeoffs between a small packet size required because of the unreliable media and a large packet size required to minimize the header overhead are considered using standard transport protocols. The choice of upper layer protocols depends on the application required to run over the network; for instance, military messaging application could use X.400 and its supporting presentation and session layers as specified in US GOSIP or the enhanced versions proposed in STANAGs 4265-4269. The paper also assesses the impact of the transport protocol selection on the network architecture in an internetwork configuration. [Ref. Bahnji 1990]

20. SUMMARY ISSUES FOR STANDARDS SURVEY

Quick Reference	
Topic	Page
Data Interchange	502
Data Management	501
Distributed Computing	505
Graphics	503
Internationalization	506
Network	503
Operating System I/F	504
Programming	499
Security	504
System Management	504
User Interface	500

This section summarizes deficiencies in standards coverage noted elsewhere in this document for the 11 service areas: programming services, user interface services, data management services, data interchange, graphics services, network services, operating system interface services, security services, system management services, distributed computing services, and internationalization. It also addresses additional areas, such as the application program interfaces (APIs) and the external environment interfaces (EEIs).

The discussion in this section is derived primarily from the NIST *Application Portability Profile* [Ref. APP 1993]. Additional information was derived from the *DoD Technical Reference Model for Information Management* [Ref. TRM 1993], and the draft MIL-STD-xxx on *OSE Profile* [Ref. JIEO MIL-STD-xxx 1992].

20.1 Software Engineering Services

Software engineering services (Chapter 4) include programming languages and language bindings and computer-aided software engineering (CASE) environments and tools.

There are international standards for most, but not all, of the commonly used programming services. Although ISO and the US Government have adopted ANSI X3.159, *Programming Language C*, there are potential compatibility problems between C and C++. The other standards are stable. However, Ada is undergoing a revision process and some aspects of the current language may not be upwardly compatible with its successor, Ada 9X. Moreover, COBOL is currently limited in real-time, operating system and communications components.

There is no standard set of guidelines for using the features of the Ada programming language; without guidance, applications written in Ada may have unpredictable portability. Ada bindings are needed for many interfaces (e.g., GUI toolkits, OSI Application Layer functionality, CDIF, SGML, X.25, TCP/IP). They have been completed for GKS (ISO 8651-3), PHIGS (ISO 9593-3), and SQL (ISO 9075:1992), and are at the DIS level for GKS-3D (DIS 8806-3) and CGI (DIS 9638-3). Ada bindings for X, SQL, and IRDS (ISO 10728 WDAM 2) are underway. IEEE P1003.5 is currently defining Ada bindings only to POSIX.1 and not to the other POSIX standards. P1003.20 is reported to be developing an Ada binding to POSIX real-time extensions.

All fourth generation languages (4GLs) are proprietary. Portability of 4GL products requires open standardization of languages and bindings.

Standards have not been developed for languages used for certain technologies and application areas. These areas might include languages used in artificial intelligence (standards for LISP and Prolog have been developed but not for other languages) and used for interfaces to specific COTS/NDI software. LISP is more popular in the United States while Prolog is more popular in the United Kingdom and Europe, posing potential interoperability problems.

Standards for software development environments, including CASE tools and environments, are in the early phases of development. Some are currently restricted to interfaces between tools while others address entire environments. Standards are needed for integrated (computer-aided) software engineering environments (ISEEs) and tools, to include systems and programs, for automated assistance in developing and maintaining software, conducting design work and analysis, creating program code, testing, documenting, prototyping, and communicating within groups. The interfaces among these tools include services for storing and retrieving information about systems and exchanging this information among the various system development environment components. ECMA's PCTE and associated reference model is widely supported by vendors in Europe. The Ada Programming Support Environment (APSE) specifications can be mapped to this reference model. The work of defining interfaces among various software components is still incomplete and in a state of flux. For example, there is as yet no consensus on the type of data model necessary to support the information structures for the environment. The extent to which environments such as PCTE and CAIS can evolve and be tailored is unknown. Moreover, CAIS is suffering from a dearth of conforming commercial products. Tool interfaces based on commercial products may lack flexibility.

Standards for KBS do not exist. Software repository standards to facilitate reuse do not yet exist. This could have an adverse effect on a COTS/NDI acquisition strategy by making NDI software difficult to identify.

Software engineering standards that address the software development process and development methods, and ultimately software quality, are in the early phases of the international standardization process. It will be at least 3 years before a foundation for these standards is established. To date, none address the development of expert systems.

20.2 User Interface Services

Of all the service groups, standards for the user interface services (Chapter 5) are the least mature. This area suffers from a general lack of standards for toolkits and UIMS and at the API level itself. API directions likely to be taken over the next 5-10 years are uncertain. GUIs remain in the research stage. Standards for window management are only emerging. While X-Windows still has not reached the stage of becoming an international standard, work is progressing. X-Windows has wide support in the United States and elsewhere, but the implementations are not standardized. Moreover, most of the X-Window functionality is available only at a low level, too low for most application programming. The Extensible Virtual Toolkit (XVT) is one of many toolkits that provide a higher level API to window system functions that is window-system independent. There are as yet no standards for the "look and feel" for application software for the upper layers (Presentation and Dialog) of the user interface system reference model (see Section 5.3).

Some issues are:

- Is there a requirement to establish a common look and feel for user interfaces? Does such a requirement come from the functional requirements, the training requirements, or from the users as a separate operational requirement?
- Is it appropriate to adopt a de facto standard, such as one set of X-Window interfaces? The user interface services area may be one case in which de facto standards must be used in lieu of international standardization.

20.3 Data Management Services

Data management services include the data dictionary/directory component for accessing and modifying data about data (i.e., metadata), the database management system component for accessing and modifying structured data, and the distributed data component for accessing and modifying data from a remote database. [Ref. APP 1993]

While the ANSI standard (ANSI X3.138-1988) and FIPS 156 are the same, ISO is working on an Information Resource Dictionary System (IRDS) specification (*IRDS Framework*, ISO 10027) that is significantly different in some respects from the ANSI standard. FIPS 156 does not completely specify interface services for a data dictionary/repository—it specifies only the user interface. ANSI X3.185 (ISO 10728), *IRDS Services Interface*, provides an API to IRDS and is appropriate for metadata interchange with a DBMS and between an IRDS and application programs. ANSI X3.195, *IRDS Export-Import File Format*, supports schema and metadata interchange among IRDS-compliant databases, among IRDS and CASE tools with repositories or dictionaries, and between IRDSs and application programs. Additional functionality is needed for IRDS, to include the capability to manage object-oriented data structures and to provide for enhanced communication of information between applications and other data management tools. A major revision of IRDS, sometimes called IRDS2, is underway and is expected to provide such functionality.

A standard relational DBMS interface is provided by *Database Language SQL* (FIPS 127-2 and ISO 9075:1992, sometimes known as SQL2), which incorporates ANSI X3.138:1989 *(SQL)* and ANSI X3.168 *(Embedded SQL)*, together with additional features for schema manipulation, dynamic SQL, exception handling, enhanced integrity constraints, transaction management, and data administration. Not yet addressed are access to remote heterogeneous sites (see below on RDA) and distributed database management. Also needed are tools for the support of object-oriented data management, such as triggers, assertions, user-defined types, domain and table hierarchies, and stored procedures. While the scope of SQL3 (whose standard is expected to be agreed in 1995) is not yet defined, it is expected to support some of these requirements.

Distributed database access is supported by *Remote Data Access*, ISO 9579. RDA is used to establish a remote connection between an RDA client, acting on behalf of an application program, and an RDA server, interfacing to a process that controls data transfers to and from a database. The goal is to promote the interconnection of applications with database systems within heterogeneous environments, with emphasis on an SQL server interface that can provide interoperability between different SQL servers. The client/server approach of RDA is one of several architectures for remote access; others may emerge in data management standards. RDA as yet only specifies the service and protocol between a single client and a single server—it does not currently specify distributed database access, nor does it support stored database procedures.

The US DoD has embarked on an ambitious program to centralize data administration and to define and adopt DoD-wide standard data elements. DoD instructions and procedures have been prepared, but most are as yet only in draft form. A DoD data repository capability has been created, but to date, only a few prime words and data elements have been approved. Development of data models (e.g., using the DoD-mandated IDEF language) for information systems has only just begun. The ATCCIS PWG has adopted and is using IDEF0 [FIPS 183] and IDEF1X [FIPS 184] in support of its process and data modelling activities.

20.4 Data Interchange Services

Data interchange services establish data formats for interchange of documents, graphics data, and product description data.

In the area of document exchange, standards exist that would fulfill an AIS's requirements. There is evidence that these standards are stabilizing as Document Application Profiles (DAPs) begin to appear. While both ODL and SGML can be used with ODA and information can be transferred between the two formats, there are some advantages to using SGML. Not only does CALS use SGML, but more commercial products are available for it than for ODL. Moreover, it is human-readable, preserves user file divisions, and is extensible to other architectures. It also possesses a broader information processing orientation than does ODL, which is concerned solely with document processing. ODA (ISO 8613:1989) models are still incomplete, and there is still ongoing work on the connection between document logical structure, layout, and content. Gaps in ODA/ODIF standards (for which future ISO work is planned) include: revision collection, status, rationale, and author information; document annotations; automatic content generation of listings such as table of contents, tables of figures, indexes, glossaries, and cross references; business charting; data in documents, such as spreadsheets; exchange of hypertext-based documents; and exchange of documents that include voice and audio information.

Central to CALS is the use of EDI (FIPS 161; EDIFACT, ISO 9735:1988; X.12-1986; ITU-TS X.435:1991) for business data interchange. EDIFACT and X.12 differ in syntax control segments, data segments, and data elements. The various versions of EDI are expected to merge (in a future edition of ISO 9735) and to use X.400-1988 messaging. An argument against using the CALS standard as a model is that it is oriented to technical weapons systems support documentation that may not be appropriate to an information system.

The status of technology in the area of data interchange is such that standards do not yet manage information as a database where content is encoded and structure and form attached.

IGES is suitable for engineering data but does not include all interfaces for use, such as the interface between the data specification and numerically controlled machining tools. STEP represents complex data objects (e.g., technical diagrams and documents) suitable for product development (e.g., for advanced manufacturing machines) from initial concept design to manufacturing and product support.

Graphics services standards all appear to be stable and mature with a high level of consensus and product availability. However, none address the question of distributed graphics. A common intermediate standard is needed to exchange graphics data stored on different platforms.

The remaining data interchange standards areas (geographic, data compression, video, and audio) are far less stable and mature. A lack of standards has impeded interoperability among digital cartographic and geographic information systems. For example, SDTS (FIPS 173) has been developed for transfer of digital spatial data among heterogeneous computer systems; however, an international forum (with the participation of the US Defense Mapping Agency) has developed an alternative specification, DIGEST. Agreement on such a standard is essential to the interoperability of geographical information systems (GISs) and between GISs and information systems (at least to import terrain data and map graphics). An information system proponent will need to monitor standards developments in these areas as well as in the area of multimedia standards where standards are generally lacking. For example, one promising technology that has been crippled by a lack of standards is multimedia mail. [Ref. Borenstein 1991]

Data compression standards, particularly JPEG and MPEG have attracted significant support, but the future has been clouded by other vendors claiming to have substantially improved technical approaches to compression.

20.5 Graphics Services

Graphics services standards all appear to be stable and mature with a high level of consensus and product availability.

20.6 Network Services

Network services can be provided for CCISs using OSI protocols for electronic mail, Directory, file management, and exchange of telematic information and documents. At the present time there are not many high-level services provided by the OSI stacks, but the communications aspects at lower layers are mature for connection-oriented services and maturing rapidly for connectionless-mode services. Only proprietary products are now available with ISDN services and protocols, and ISDN usage is not yet widespread in the United States. IEEE has developed a draft standard (P1003.8 Draft 6) for Transparent File Access (TFA). TFA-like features are available in several products, but there is as yet no common specification for such file system semantics.

Analysis is now being performed in TSGCE SG9/WG2 to identify additional features required for military application of MHS (see Section 17.3.4.2). Analysis of the relationship of MHS to ACP 129 and ASN.1 to STANAG 5500 and other message standards is needed. NATO has requirements for media independent data communications protocols (e.g., for Link 1 replacement) that have not yet been developed; these standards could be applicable to the communications services, and more work needs to be done in this area.

In a comparison of the 65 service elements of ACP 127, a recent analysis [Ref. USPR 1989] has identified 55 as common to MHS-88. An additional five service elements were shown to be related to, but not the same as, those in ACP 127:

- Precedence levels (MHS-88 provides an Importance Indicator)
- Message identification (MHS-88 provides somewhat different features)
- Prosign C (MHS-88 has an obsolescence indication)
- Bell signal (MHS-88 provides a stored message alert)
- Date-time group (MHS-88 has a submission time stamp).

Five services provided in ACP 127 are not supported in MHS-88: financial accountability, service message, network continuity indication, off-line accountability, and tracer action.

ISO SC21/WG1 is still refining the OSI Reference Model regarding the specification of the boundaries of Layers 1 and 2. Some of the protocols needed for the communications services may be determined to lie outside the Reference Model. These might include forward error correction coding[152] (several ISO standards provide for error detection) and other mechanisms such as interleaving of bits from a sequence of octets to reduce the impact of the environment on certain transmission media. Protocols for handling requirements of cryptographic devices (e.g.,

152 Whether forward error correction (FEC) is outside of the OSI Reference Model is still a contentious issue in ISO, US PSSG, and NATO. Valid arguments exist for FEC at either Layer 1 or Layer 2.

synchronization) and media access may also lie outside the Reference Model. Standardization of these features should, wherever possible, be accomplished with media-independent standards.

20.7 Operating System Services

Operating system services include kernel operations, commands and utilities, system management, real-time extensions, and security. Four of these areas (management is excluded) are addressed by POSIX. The POSIX standard provides the broadest applicable reference model for developing portable applications at the source code level. Considerable progress has been achieved, and there is additional work in process. [Ref. OSN 1993h]

Standardization of operating systems appears unlikely. Further, there is no need to select a standard operating system for an automated information system, since such a selection is viewed as an implementation issue. When mature, adopting the POSIX interface standard for information systems appears to be an attractive option, both to achieve some of the required system services and to promote applications portability during implementation. Adoption of the current POSIX standard would probably not fully meet system service requirements. For example, POSIX addresses independent operating systems cooperating in a distributed environment, not a single operating system running on multiple machines. It is not specifically designed for distributed applications, and therefore may not serve an information system's needs completely.

Moreover, IEEE 1003.1-1988, *System Application Program Interface* (FIPS 151-1 and ISO 9945-1) does not include the capabilities for kernel security that are typically provided in an operating system kernel. Also required are real-time profiles (IEEE P1003.13) and testing specifications.

Recent developments at X/Open concerning the UNIX API also bear watching.

20.8 Security Services

While there is a great deal of activity in standards for security services, there is very little that is complete. The most mature technical areas are operating system and physical layer network standards, but even here the standards are not mature. Security in most other aspects still contains areas of basic research. The standards that have been approved are generally the umbrella standards, such as ISO 7498-2.

20.9 System Management Services

Quality of Service and security are not well addressed by OSI and other open systems standards. Both of these sets of services require review and possible modification of the basic reference models for open systems. They therefore could lead to disruption of some of the standards that have already become stable under the existing reference models.

Both sets of services may be supported in a wide range of ways, and several approaches of these may be required in information systems to meet operational requirements. For example, quality of service affects all the layers of the OSI Reference Model, and the associated protocols, managed objects, and parameters of the protocol data units may all have to be extended to meet military requirements. Security can be expected to impact at least the Physical, Network, and Applications Layers of the OSI Reference Model (the NATO position) and other layers as well (SDNS also provides a protocol for the Transport Layer).

Work has already begun on OSI services and protocols in the management area. Systems management is generally acknowledged to affect all service areas, especially operating system

services and network services. The only consensus achieved to date for standardizing systems management services is in the OSI network management area. Version 1 (June 1992) of the Government Network Management Protocol (GNMP) identifies information required for managing implementations incorporating network services only at the Physical and Data Link Layers, and it does not provide a complete set of managed object definitions or the necessary security features for network management.

Support for access control and authentication is already being incorporated into a number of OSI standards. Many other aspects of security, such as key management, still must be standardized to ensure interoperability and to avoid building the same functions many times in similar systems (e.g., function-specific information systems) and in the applications of a single system, such as a CCIS.

Management issues can be expected to differ for each of the technologies being considered for information systems. For example, security aspects of local area networks differ from those associated with broadcast radio and packet-switched point-to-point links.

Findings in security and OSI management are:

- Standards for OSI security are evolving, but the evolution is slow. OSI standards may not be satisfactory in some areas (e.g., OSI services) in and of themselves for military applications. They may need to be supplemented by application-level services outside the OSI model.
- An adequate treatment of management services may require modification to the OSI Basic Reference Model and thereby impact many stable OSI standards.
- Some management standards are now stable (e.g., ISO 9595, ISO 9596; ISO 10040, ISO 10164, ISO 10165), but there is standardization required in many additional areas.

20.10 Distributed Computing Services

The effort that OSF has put into DCE is beginning to mature. The technology will be widely available in the first half of 1994. Most major open systems vendors will offer a version interoperable with the others on their UNIX based systems. Many will also feature DCE ports on their proprietary systems, for example IBM's OS/2. SUN and Microsoft may be the only exceptions; however TRANSARC will provide a version for Solaris, and Gradient Technologies will provide a version for Microsoft Windows.

In terms of de facto standardization, UNIX International has promised to provide DCE Compatibility in the near future; Siemens already provides a System V Release 4 version of DCE as an OSF Reference Model. X/Open is "fast-tracking" DCE for incorporation into its next version of XPG. After being "standardized" by X/Open and adopted by the open system vendors, actual ISO or ANSI standardization will not be far behind.

The current version of DCE appears to be usable for unclassified uses. Care must be exercised if it is to be used for classified uses. The next year will see the definition of a generalized security API for DCE, which will aid the implementor in developing applications that deal with classified data. Few applications utilizing DCE exist. Developer kits and the standardization of the application environment will help to provide the impetus so that applications using the interfaces should begin to appear late next year.

One of the most demanding application suites, the Distributed Management Environment 1.0 has just been released to vendors. DME must still be tailored to the DCEs of

individual manufacturers. Printing services and their management will not be provided until this spring. The management framework is not due until late in 1994 or early in 1995. Complete management services based on an integrated set of services from DCE and DME are not likely until mid-1995 at the earliest.

This could be hastened if the deployment of the OMG Object Request Broker and the dependent services is speeded. Currently a number of manufacturers have ORB products available. The new version of the ORB, which emphasizes interoperability, is not yet available. One might expect its specification in 1994 with implementations in early 1995. The ORB and its associated suite of object services should be available in late 1995 or early 1996. These services, which could be based on DCE, could stimulate the development of distributed services and applications. If kept on track, DCE, DME, and the ORB should enable the high volume production of applications by 1997.

20.11 Internationalization

In the area of Internationalization, the character set work is the most mature. Some industry actions have also occurred. MKS has announced fully internationalized and multibyte-enabled versions of its InterOpen source code products. These are InterOpen/Multibyte POSIX shell and utilities, InterOpen/Multibyte SPG4 commands and utilities, and InterOpen/Multibyte XPG4 terminal interface. Single byte internalization allows text messages, input, output, and data processing to occur in most languages for which a single byte character set exists—such as French, English, and German. Multibyte internationalization extends this to accommodate large repertoire languages such as Japanese and Chinese, while maintaining support for single-byte languages. IBM is the first company to license the internationalized version of InterOpen/POSIX shell and utilities, and implements this source code on its mainframe operating system OpenEdition MVS.

APPENDIX A

OVERVIEW OF THE ATCCIS ARCHITECTURE

OVERVIEW OF THE ATCCIS ARCHITECTURE[1]

The purpose of this appendix is to provide a technical overview of the ATCCIS architecture. However, this information is not required to understand the review of standards that follows. For more information on ATCCIS, the reader should first consult the ATCCIS *Phase II Final Report* (October 1990), the *Phase III Work Plan* (December 1991), and the *Phase III Project Brief* (December 1991), from which this overview is taken [Refs. ATCCIS 1990, ATCCIS 1991]. Table 1 identifies the ATCCIS documents that have been circulated to the Nations by SHAPE.

1. BACKGROUND FOR ATCCIS

1.1 ATCCIS Purpose

The primary purpose of the ATCCIS program is to achieve interoperability between national automated CCISs for use in the Central Region (CR) at Corps and below in the years 2000 and beyond. Two implicit objectives are to ensure that (1) ATCCIS-conformant systems deployed by the Nations are also interoperable with the systems being developed under the Allied Command Europe (ACE) automated CCIS programme and (2) such systems are affordable.

The ATCCIS Permanent Working Group (PWG) was tasked by Supreme Headquarters Allied Powers Europe (SHAPE) to develop an operational and technical concept for an interoperable tactical ACCIS that is based on stated operational requirements and evolving military concepts. The PWG is comprised of army officers and civilian scientists from seven Nations (Denmark, France, Germany, The Netherlands, Spain, United Kingdom, United States), SHAPE, and Allied Forces Central Europe (AFCENT) (with Canada and Italy as observers) working cooperatively in accordance with guidance from SHAPE.

1.2 ATCCIS Objectives

To satisfy the primary purpose of attaining interoperability, the ATCCIS development programme must satisfy four principal objectives:

1 Extracted from the ATCCIS Phase II Final Report [ATCCIS 1990].

a. To formulate common requirements for the use of battlefield information
b. To ensure that all international and multinational users of critical battlefield information can exchange that information on a basis that is mutually agreeable
c. To exchange information so that it conveys the same meaning and understanding to source and recipient alike
d. To define a technical architecture capable of accomplishing the necessary exchanges and transactions.

Table 1. Listing of ATCCIS Papers Distributed by SHAPE

No.	Class	Title	Edition	Date
-	NU	Phase II Work Plan	2.0	Sep-86
1	NS	Threat	1.0	Mar-86
2	NR	Mission Needs & Objectives	1.0	Sep-85
3	NC	Concept for Survivable C2	1.0	Dec-87
4/5	NC	Key Tasks	1.0	Oct-85
6	NC	Echelons & Staff Organizations	1.0	Jul-86
7B	NU	Degrees of Data Interoperability	1.0	Mar-86
7F	NU	Databases	1.0	Aug-89
7L	NU	Data Management & Standardization	1.0	Jun-89
7M	NU	Methodology for Identifying C2 Operational Requirements	1.0	Sep-89
7N	NU	Standardization of Data for Interoperability	1.0	Sep-90
8	NC	Operational & Functional Concepts	2.0	May-88
10	NC	Information Flow Requirements & Products for Each Key Task	2.0	Sep-90
11	NU	Requirements from Key Tasks	2.0	Jan-90
12	NR	General Requirements	1.0	Sep-88
12A	NR	Security Requirements	1.0	Sep-88
13	NU	IERs Among Elements of Each HQ	1.0	Feb-88
14	NC	IERs Between HQs	2.0	Sep-90
17	NC	Interfaces to Non-ATCCIS	1.0	Apr-88
18	NR	Operational Standards for ATCCIS IERs	1.0	Sep-88
18A	NU	Modernization of Land Force Operational Standards	1.0	Sep-89
22	NU	Architectural Concepts	3.0	Sep-87
23	NU	Requirements Analysis	1.0	Sep-87
24	NU	Architecture Definition	3.0	Oct-90
24B	NU	Properties of TF and SCF	1.0	Dec-87
25	NU	Technical Standards for ATCCIS Architecture	3.0	Jan-92
30	NU	Applicability of the Architecture	1.0	Jan-90
34	NU	ATCCIS Communications	1.0	Jan-90
34A	NU	Background to ATCCIS Comms	1.0	Oct-88
39	NR	Phase II - Final Report	1.0	Oct-90
-	NU	Phase III Work Plan	1.0	Dec-93
-	NU	Phase III Project Brief	1.0	Dec-93

1.3 ATCCIS Phase II Findings

There were eight principal findings of the Phase II study.

1. **There is more than 80% commonality in the key command and control (C2) tasks performed at corps level and below**, despite the fact that the organization and structure of command posts (CPs) utilized by the four Nations differ significantly.

a. The PWG developed and harmonized a detailed listing of the Key Tasks performed at tactical echelons by the ground forces of each of the four Nations. The PWG also documented the specific information needed by a particular command or staff element/cell in order to accomplish a given Key Task. These analyses demonstrate that the Nations have common requirements for the use of battlefield information.

b. CR Nations do not have a common way of expressing their operational requirements when participating in multinational cooperative C2 efforts. Therefore, the PWG adopted an ACE methodology, Command and Control Requirements Analysis (C2RA), and successfully modified it for use at the tactical level. It appears that this method is suitable for adoption by other Nations faced with a similar requirement. Indeed, the ABCA (Australia, Britain, Canada, and America) Nations have adopted the ATCCIS methodology as their way ahead for progressing C2-related projects.

2. The four Nations can directly correlate those specific C2 processes performed in, and the information exchange requirements (IERs) pertaining to, their respective corps, division, and brigade CPs with a harmonized set of ATCCIS C2 processes and sets of ATCCIS IERs.

a. The forces of all Nations must have a common understanding of how C2 processes are performed in order to operate effectively together and ensure that orders and directives are not misinterpreted. Notwithstanding national variations in organization and doctrine, the detailed analyses revealed that the C2 processes carried out by all four Nations are essentially common. The study represents the first comprehensive investigation of the essential and necessary interactions between the national formations and NATO Principal Subordinate Commands (PSCs).

b. The study effort identified the producers and users of nearly 3,000 C2 Products such as operations orders or situation reports. Using these results, the IERs were then defined for those national forces that might be required to operate in coalition with the forces of other Nations or under the operational control of a NATO Headquarters (HQ). Requirements have been reconciled with the emerging results of the ACE ACCIS system design and integration effort.

3. Current C2-related operational standards prescribed for use by NATO and the Nations are often conflicting, inadequately defined, and ill-suited for international exchange of information in either a manual or an Automatic Data Processing (ADP)-supported CCIS environment.

a. NATO C2-related operational standards have been compared with corresponding national instructions, doctrine, and directives. It was found that many of the standards are out-of-date or imprecisely written. In other instances, individual Nations and formations have opted to implement modifications that no longer resemble the base standard. This is an unsatisfactory basis for progressing either manual or ADP-supported CCIS programmes.

b. To remedy this problem, the PWG proposed a strategy for modernizing NATO C2-related operational standards. SHAPE endorsed the PWG proposal and forwarded it to the NATO Military Agency for Standardization (MAS). More work is urgently required before this problem can be rectified.

4. A NATO-wide data management policy is required.

a. The need for such a policy is well established in NATO, but none has yet been promulgated.

b. Commonly agreed and unambiguous definitions of data are required for use in ACCISs. Lack of such definitions severely inhibits the attainment of international as well as multinational interoperability. Current operational and technical procedures cannot ensure that the source and the recipient of information that is exchanged between and among cooperating formations will each share the same meaning and intent of that information.

5. A technical architecture for an ATCCIS can be defined by using international commercial (nonproprietary) standards supplemented, where necessary, with military enhancements or standards.

a. Given the existing significant differences in national philosophy, organizations, funding, and procurement schedules, it was determined that development of common hardware for ATCCIS would not be practical.

b. The PWG determined that the most feasible way for the technical work to proceed would be to focus on the establishment of an architecture that would provide a common basis acceptable to all Nations.

6. The analysis has concluded that an ATCCIS-conformant system must be a transaction processing system with a partitioned, partially replicated database.

a. The essential nature of military C2 is the interaction of commanders and their staff with superior and subordinate formations, by the manipulation of military information through various forms of transactions.

b. ATCCIS-conformant systems must be capable of supporting applications and maintaining the capability for consistent interpretation of data across national and multinational formation boundaries.

c. The interactions that users of tactical ADP systems make are in the nature of transactions that are, for example, in the form of updates to a database, requests for information, or orders to be issued where appropriate. Future demands on transaction processing systems will probably take the form of decision support.

d. The architectural concept is defined in terms of a number of logical facilities that provide technical services essential for the interoperability of ADP systems that support the C2 function. The key attribute of ATCCIS-conformant systems is Basic Interoperability, i.e., the exchange of information that preserves the meaning and relationships of the information exchanged. It is achievable through the implementation of four facilities; the facilities themselves are defined in terms of standards, protocols, and functionality. However, it is still too early to select specific interoperability parameters, individual standards, or stacks of standards.

e. The sole requirement placed on tactical communications by the architecture is to provide a standard network service.

7. The concept for the ATCCIS architecture is consistent with that for the NATO Consultation, Command and Control (C3) Architecture.

a. The current NATO C3 Architecture draws heavily on ATCCIS technical proposals.

b. The ATCCIS technical concept is also compatible with the draft guidelines for technical standards being established within NATO.

8. Operational and technical standards necessary for national implementation are still immature; a programme definition phase is required.

1.4 ATCCIS Method of Work for Technical Analyses

The technical analyses in ATCCIS have been limited to those aspects of the architecture that appeared to be essential to achieving basic interoperability--the exchange of information that preserves meanings and relationships--and the potential for cost savings without unnecessarily limiting national implementation options. Provision has been made in the proposed architecture for supporting a wide range of approaches for developing and implementing applications to support operational requirements, but there was no attempt to delimit or specify those approaches. Technical and procedural standards were reviewed for their applicability for specifying the architecture, but no selection of such standards has yet been attempted. The review has identified standards employed in NATO and--where such standards could be widely used--in the Nations for ensuring interoperability and providing the potential for cost savings. Preliminary analysis has been performed on the applicability of the architecture to a wide range of operational configurations, but this analysis was descriptive rather than complete in so far as covering all possible operational requirements or in fully validating the technical aspects of the architecture. Technical analyses have also addressed the impact of the architecture on communications and of communications on the architecture, but it is too early to be definitive about what communications will be in place by A.D. 2000.

Key features of the technical approach can be summarized as follows:

- *The architecture was specifically limited to defining only those aspects required for interoperability.* The architecture is not intended to be a complete architecture satisfactory for implementation. Specifically, the architecture does not define any application-level facilities, nor does it define any user interfaces or user interaction with the database.
- ATCCIS conformancy limits implementations only to the extent that they must provide the services and logical facilities of the architecture. Thus, the architecture intentionally does not have the detail required to guide the choice of computer architecture, workstations, operating system, database management system, or other commercial off-the-shelf (COTS) products. These aspects, together with the definition of application-level facilities and user interfaces, would be national options and would have to be addressed in national systems.
- The architecture is, by design, driven primarily by the requirement for interoperability. National CCIS architectures are expected to differ depending on the additional driving requirements imposed to meet national needs, which include the use of COTS software, support common software development among several Nations, or use a wide mix of products from different vendors.
- NATO has defined six "Degrees of Interoperability," reflecting the procedures by which the transfer of data associated with interoperability is to be achieved. It has been generally accepted that degree 5 interoperability--automated data exchange with user-imposed access restrictions--is the mechanism required by the Nations and has been adopted by the study as the basis for providing interoperability. Many of the concepts underlying the architecture are governed by the requirement to implement degree 5 interoperability.

2. Fundamental Concepts of the ATCCIS Architecture

This section describes seven concepts that are fundamental to the architecture.

2.1 Information Exchange

Information Exchange Based on Information Items. Information items are the essential ingredients for the performance of a military Key Task (both input and output). Information exchange today is conducted on the basis of formatted messages in the form of C2 Products, which ideally are composed of agreed groups of information items. However, in the future, information exchange between conformant systems will be conducted on the basis of information items themselves, and the required information aggregates can be constructed from these information items. Information products in their entirety constitute a highly inefficient basis for information exchange. Note that:

a. Preparation of information aggregates from groups of information items in performance of Key Tasks is the prerogative of national implementation and may not necessarily be standardized.

b. The definition of information items that support the performance of Key Tasks is seen as relatively stable, whereas the procedures for performing the Key Tasks and the form of the associated C2 Products can be expected to change more often.

c. Agreement on the exchange of information items that preserves meaning and relationships is essential for interoperability, but agreement on formats for presenting these data is not required for interoperability.

d. A C2 Product may be propagated by creating a new set of its constituent data items. However, a C2 Product may also be propagated more efficiently by an update to some of its constituent items.

Information Exchange Based on Other Data Types. Information will need to be exchanged for other types of information objects--an object contains information in some agreed context--than objects based only on information items for structured data. Examples of such information objects are assessments, briefings, documents such as operations orders, video imagery, graphical displays such as map overlays, and terrain representations. Document exchange can be achieved by agreements on document structure and format without restricting national options for implementing word or text processing capabilities or national preferences for how documents are presented to users.

2.2 Information Models

The architecture will need to support several types of data models, including a relational model for a database for structured data. Since structured data is expected to be present in all ACCISs, the relational model will be common to all conformant systems.

Relational Model. For many army ACCISs, data are distributed and selected parts of the total data are replicated in a limited number of locations; this is a concept technically referred to as a partitioned, partially replicated database. Since data are maintained in a number of locations because the data originate and are used in different locations, the connectivity of those locations cannot always be guaranteed. Unexpected temporary or permanent loss of nodes and links is a feature of the military environment. Furthermore, communications limitations may demand local caching (storage) for performance reasons. Hence, *in order to ensure that the required data is available at a specific location at the time it is needed, the database is organized and maintained as a partitioned, partially replicated database.*

Other Data Models. *The architecture will need to support information models other than the relational model described above.* These could include object-oriented models for such data types as documents, imagery, and terrain representations. Further, the architecture will need to provide for the integration of different types of data (e.g., data items or documents) for the various models. Each data model will lead to a different type of database in an implemented system.

2.3 Information Transfer

Three criteria have to be satisfied in order that Basic Interoperability can be achieved:

- Transfer of Data. There must be a means whereby data can be physically moved from the originating HQ to another HQ that needs that data.
- Interpretation of Data. There must be some means of identifying the data so that the two (or more) HQs using the data can be certain they will all interpret it in a consistent manner.
- Management of the Basic Interoperability Functions. There must be mechanisms for managing the processes involved in these operations, including (but not restricted to) the needs for security and keeping abreast of a changing tactical disposition of HQs.

The minimum capabilities required to support these criteria are (1) a mechanism that provides end-to-end transfer of data, (2) a mechanism to manage the storage, retrieval, and interpretation of data, and (3) a mechanism that manages these two mechanisms.

Several types of transfer mechanisms may be required for the various data types. Database-to-database transactions could support transfer of structured data (defined, for example, by a relational information model). Other transfer mechanisms may be required for exchange of such data types as documents; candidates are file exchange, military message handling, or electronic mail.

2.4 Transaction Processing

The interactions between users and an ACCIS are in the nature of transactions (e.g., in the form of updates to a database, requests for information, or orders to be issued). This transactional characteristic of ACCISs will continue to apply in the future with the expectation that there will be additional demands on such systems, for example, in the form of decision aids and other forms of automation to support the decision process. Therefore, *the principal characteristic of systems that support tactical C2 is transaction processing.*

2.5 Support for Applications

Requirements have been identified for providing military services to users, which in turn require the provision of decision support and other functions to support the performance of Key Tasks. The provision of these functions will be fulfilled by a set of applications executed on the ADP systems supporting the staff in the performance of their Key Tasks.

It is therefore necessary for conformant systems to be able to support the execution of such applications. Furthermore, the allocation of applications to particular systems or parts of systems should not be fixed, but should have sufficient flexibility to allow for changing operational situations. The manner in which such applications are incorporated into a system is specified by the architecture, but the detailed specification of the functionality of any particular application is outside the scope of the architecture and may be a matter for individual Nations to determine for themselves, or may be the subject of separate multinational agreements. Within the architecture, any application, irrespective of its functionality, must conform to certain rules and interface standards.

2.6 Support for Human-Computer Interfaces (HCIs)

The technical capabilities of a system, and the information held within such systems, are of no practical use unless the staff users can gain access to those capabilities and information. It is therefore essential for systems to provide an adequate human-computer interface. Agreement on a common human-computer interface is not essential

for interoperability and is therefore not addressed as part of the requirements for Basic Interoperability. However, there are many benefits to be obtained by adopting a common approach to human-computer interface, including, for example, a common presentation to users and the potential for common development of software for applications. The architecture therefore has identified in outline a Man-Machine Interface (MMI) Service Facility (MSF) to provide a common set of services. Such a facility allows the adoption of a User Interface Management System (UIMS), providing such capabilities as window managers and user dialogue managers to allow flexibility for applications while at the same time removing from those applications the need to account for the particularities of any one set of equipment for user interaction.

2.7 Information Exchange With Nonconformant Systems

Interoperation with nonconformant systems will be an important capability of conformant systems during the transition phase. In addition, it is expected that there will always be some nonconformant systems fielded by the Nations; information exchange with those systems is expected to be in accordance with current NATO procedures that use message text formats (i.e., STANAG 5500). Such systems may be manual or ADP-supported, and the degree of interoperability achievable and the services required may cover a wide range. An additional set of facilities has been identified to provide for such interoperation, although no detailed effort has been allocated to refining their specifications. *In order to achieve interoperability with nonconformant systems, there must be an agreement on data standardization.*

3. Overview of the Architecture

The fundamental concepts on which the architecture is based are identified in Section 2.4 and describe a transaction processing system with a partitioned, partially replicated database, capable of supporting applications and maintaining the capability for consistent interpretation of the data across organizational boundaries. This description of the nature of an ATCCIS-conformant system is basic to the structure of the architecture.

The architecture is defined in terms of a number of facilities (defined below) essential for the interoperability of ADP systems, which support the command and control function and provide opportunities for cost savings. The facilities are themselves defined in terms of functionality, protocols, and standards.

4. ATCCIS Facilities

A facility is a logical entity that provides at its external interface a set of related services, which includes all of the functionality necessary to provide those services, together with any additional functionality required to relate one service to another or to maintain the status and internal logical properties of the facility. The architecture defines the logical structure of, and interrelationships among, the facilities. The facilities necessary to provide Basic Interoperability are referred to as the Basic Facilities, whose functionality must be standardized for all conformant systems.

4.1 Basic and Application-Level Facilities

There are four Basic Facilities in the ATCCIS architecture:

(1) Data Management Facility (DMF). The DMF provides functionality to ensure the proper management of data, and to ensure that there is a consistent representation of data and data relationships across all conformant systems.

(2) Transfer Facility (TF). The TF provides functionality to allow different parts of a system, or two conformant systems, to invoke services one from another. TF includes data transfer protocols, services of the communications infrastructure, and services to manage data transfer and communications.

(3) System Management Facility (SMF). The SMF provides functionality supplementary to the management services of the TF and DMF for control of part or all of a system.

(4) Service Control Facility (SCF). The SCF provides functionality to control interactions among all other facilities.

The Basic Facilities provide the three mechanisms identified in Section 2.2.3 (viz., providing end-to-end transfer of data; managing the storage, retrieval, and interpretation of data; and managing these mechanisms) as the minimum capability to support Basic Interoperability.

Application-Level Facilities (ALFs) provide the functionality associated with performing the automated parts of Key Tasks in a subfunctional area (SFA). Within the architectural model, there may be some ALFs

providing general application-level services common to a number of subfunctional areas or Key Tasks, and other ALFs providing particular functionality in support of one SFA or a single Key Task. The extent to which Key Tasks in an SFA are supported by automation is a national prerogative. ALFs could be national-unique, standardized among some nations, or standardized among all the nations.

4.2 Other Facilities

Two additional facilities have been identified for the architecture, other than the ALFs and the four Basic Facilities. These are the Man-Machine Interface (MMI) Service Facility (MSF) and a family of Input/Output Facilities (IOFs). The MSF provides the functionality for a generalized interface between ALFs and users, irrespective of the particular devices used to interact with users and the human-computer interface they implement. Each IOF provides an interface between a conformant system and a particular class of nonconformant systems. There are as yet no formal operational requirements for the MSF or IOFs, but agreements to standardize these facilities could lead to opportunities for cost savings.

4.3 Facilities and Operational Activities

Four classes of activities have been identified in the operational analysis of Key Tasks (WP 11) that need to be supported by ADP functionality. These classes and their relationship to the facilities are as follows:

- Access. This class includes all activities and actions involved with the access by the user to information, or recording information provided by the user. It includes any subsidiary activities and actions to enable the user to specify and carry out his access requirements satisfactorily. In this context for an ADP system, the term "user" should also be interpreted as including any item of software operating on the user's behalf. The access class will be provided primarily by the DMF, supported by human-computer interfaces (e.g., MSF), and ALFs.
- Processing. This class includes all activities and actions involved in the manipulation of information to produce new, or revised versions of existing, information. The processing class will correspond to the functionality associated with performing the automated parts, if any, of Key Tasks in an SFA. Within the architectural model, there may be facilities providing general application-level services and facilities providing particular functionality in support of one SFA or a single Key Task. This functionality will be provided through ALFs. There may be a significant number of processing activities and actions performed manually.
- Transfer. This class is specifically concerned with the transfer of information from one command post or group of users to another. It is not concerned with any processing of the information, nor with the presentation of the information to the user, nor recording updated information that the user might provide. Again, in this context for an ADP system, the term "user" should also be interpreted as including any item of software operating on the user's behalf. The transfer class will be primarily provided by the TF and DMF.
- Control. This class includes all activities and actions concerned with the management of the C2 process, rather than performing specific actions within the process. The control will be supported by the management services of TF and DMF, the SMF, and ALFs with specific system management functionality. Interactions among the other facilities will be controlled by the SCF. There is expected to be a significant number of control activities and actions performed manually.

4.4 Interaction Between Facilities

Each facility will provide a defined set of services. These services are available to all other facilities within the same ensemble (see below). A facility that calls on the services of another facility must do so by means of a predetermined service call with a predetermined set of parameters. The service requested may provide an acknowledgment, a return of data, or both, or an exception condition. The action of the called facility will be predetermined.

5. Ensembles and Components

5.1 Basic Ensemble

An ensemble is a set of facilities that includes, as a minimum, the four Basic Facilities. The smallest ensemble is one that contains only the Basic Facilities and is referred to as the Basic Ensemble. A set of facilities

that does not include the four basic facilities (i.e., does not include the Basic Ensemble as a subset) is not an ensemble; it is merely a grouping of facilities that has no significance.

Systems may be represented logically as configurations of ensembles. Two ensembles participating in a peer interaction may be part of the same or different systems. The TF provides, by virtue of its functionality, the linking mechanism between all ensembles.

A simplified picture of the architecture is depicted in Figure 3. It shows the relationship between the TF and the other facilities in two ensembles. The Basic Ensembles are highlighted with bold lines. SMF, SCF, and DMF each appear in all the ensembles, whereas the TF is considered common to all the ensembles. Ensembles A and B can be thought of as the facilities at two physical locations. The TF includes the services for open systems interconnection and the bearer circuits (i.e., communications media).

5.2 Interaction Between Ensembles

The TF links one ensemble to another. A facility in any ensemble has access to the TF. Facilities may call on the services of other facilities that form part of the same ensemble for assistance. A facility will be aware of the other facilities within its own ensemble, but will not, in general, be aware of the existence of other ensembles. However, a facility can be made aware of other instances of the same facility that exist in other ensembles, known as peer facilities, and can interact with those peer facilities through the functionality of TF to assist in providing its services. For example, data replication and remote access to data both require peer interactions between data management facilities. A facility will not normally be aware of the existence of the same facility in every other ensemble; indeed, restriction on the awareness of other ensembles will be one of the mechanisms employed to control access and "need to know."

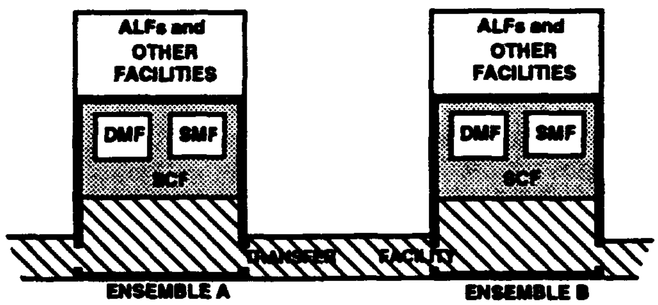


Figure 3. Facilities of the Architecture

A facility requiring services from another ensemble may call only on the services of a peer facility. If the services of a different type of facility are required, the calling facility must call on the local instance of the called facility; in the absence of such a local instance, the services of that facility are not available.

5.3 Components and Their Relationship to Ensembles

A Component is a collection of hardware and software that implements, as a minimum, the Basic Facilities in order to interoperate with other Components at least at the level defined by Basic Interoperability. It must provide the services of those facilities, either by implementing all of those services itself or by providing access to their implementation on other Components.

There is a one-to-one relationship between Components and ensembles. Specifically, the implementation of an ensemble is a Component, and a Component implements only one ensemble. The subsets of an ensemble, even if they include the Basic Ensemble, are not thought of as separate ensembles in relation to the Component on which they are implemented. Thus, consolidating the facilities from two Components onto one Component, as may be required if one of them becomes inoperative, is considered as combining the two ensembles into one ensemble, not implementing two ensembles on one Component.

A collection of Components is known informally as a system, usually with a qualifier that indicates the basis for the collection, such as a headquarters system or a national system. There is a wide range of possible configuration options for a headquarters system, from a single Component serving all users through terminals to a large number of individual workstations, each a Component, interacting to provide the total requirements of the HQ.

It should be noted that a set of workstations connected on a LAN may be a single Component or each workstation may be a separate Component, depending on whether the four basic facilities have been implemented once for the collection or once in each workstation. The choice is entirely a national option. In the case where each workstation is a separate Component, it is likely that the measure of interoperability among such a grouping of ensembles will be significantly higher than the measure of interoperability specified overall. This is also a national choice. Thus, system specifiers are free to determine their requirements independently for local interoperability.

Automated support of subfunctional areas will be implemented on a set of Components. Data elements owned by those subfunctional areas will be managed by DMF services implemented on those Components. Those DMF services must ensure that these data elements are available to the other subfunctional areas that require them. An SFA may not create, delete, or amend data elements owned by other subfunctional areas.

5.4 ATCCIS-Conformant Systems

If a number of Components are interconnected according to the architectural rules, then the resulting system itself becomes conformant. A conformant system will, in general, comprise a number of distinct interconnected Components, each of which must conform to the architecture and interoperate with other Components of the system, and with Components of other systems, according to the standards defined by the architecture. Thus, the conformance of a system can be demonstrated by proving all its Components and interconnections to be conformant. A conformant system will remain conformant if additional conformant Components are connected according to the rules and standards defined by the architecture. From a technical point of view, when two systems are interconnected they can be considered as a single system. However, management considerations will normally differentiate between the two systems.

An HQ will be configured from one or more Components. A Component may host part or all of one or more subfunctional areas. Implementing agencies would have great freedom in how the software and hardware of a system might be designed to achieve conformancy.

5.5 System Management

Services must be provided to allow conformant systems to be configured and managed so that users' ADP needs are satisfied in the most effective manner. System managers will call on system management ALFs to assist them in managing the system in the same way that other users will call on their specific ALFs to perform their day-to-day roles.

Several aspects of a conformant system will require data to relate its own operations to other parts of that system or to other conformant systems. Some Key Tasks are concerned with system management and will manipulate sets of information containing system management parameters. System management information exchange requirements (IERs) define the exchange of system management parameters. Tables of system management parameters will be managed by the DMF with access rights specific to the system management functions. Users, other than system managers, will be able to read but not modify these tables.

An example of a system management table is the logical-to-physical translation table that will be used by the TF.

Other aspects of system management will be performed by the system managers calling on management services of the DMF and TF. Most of the system management functions, which will be offered to the system managers as high-level services by the appropriate ALFs, will be effected either by these local system management services in TF and DMF or by the maintenance and distribution of local tables.

6. The Four Basic Facilities

This section provides technical details regarding the four basic facilities: DMF, TF, SCF, and SMF.

6.1 Data Management Facility (DMF)

The purpose of data management is to (1) represent the meaning and relationships of the information items required to perform key tasks, (2) ensure meanings and relationships are preserved when information is exchanged with another conformant system, and (3) ensure changes to data items are applied consistently wherever these items are stored. The DMF needs to support a number of data models, including a relational model for structured data. These data models should be derived from a common conceptual schema to ensure compatibility of the data objects and data elements.

Requirements. The DMF is required to provide data from the ATCCIS database to a facility in the same ensemble performing a service on behalf of the user. Further, the DMF supports updates to the database, replicates a partition between ensembles, and copies a partition for local use.

Concepts. A replication domain (RD) is a partition of the data owned by an SFA. The RD is the smallest unit of the database that can be replicated in full. An RD contains data from a single data model.

A replication pattern is a specification of which ensembles are permitted to hold a copy of an RD other than the ensemble owning the RD. The replication pattern is one of the mechanisms for providing access control in the architecture.

An access control domain (ACD) is a subset of an RD with a common set of authorized users. A set of data elements, in the case of structured data with a relational model, comprises an ACD.

Services. There are three primary services provided by the DMF: update transactions, access, and replication transactions.

- Update transactions are performed on RDs in a single ensemble. (As a national option, within the same HQ one update transaction may update RDs in multiple ensembles.)
- Access is the retrieval of a set of values for specified data elements (or other data objects). Access may be performed by:
  (1) Query, from an RD in the same ensemble as the requesting facility
  (2) Remote query, from an RD in another ensemble to which access has been previously agreed.
- Replication transactions copy all the data that has been updated within the RD to another ensemble. The services provided by a replication transaction may depend on the type of data in the RD.

By definition, the physical manifestation of a source RD for a replication transaction is in a single Component and the physical manifestation of the target RD is also in a different single Component. Thus, since the physical manifestation of an RD would be entirely contained in the database (or other appropriate data structure implementing the data model) at a single Component, the protocols for a replication transaction are simpler than if the replication involved sources or targets with multiple databases spanning several physical Components. A complete list of DMF services is provided in Annex A of WP 24.

Support for DMF Services. A special RD (called a system management RD) will be defined to describe the RDs accessible to each DMF and to identify the logical addresses of the physical manifestation of those RDs.

DMF Services are Transparent to the User. All data to which the user has access are in the ACDs of RDs known to the DMF. Some of that data will reside locally (in the same ensemble as the DMF) and some remotely (in an ensemble of another Component). Speed of access performance may depend on whether the DMF needs to invoke a query or remote query to satisfy an access request.

The DMF can be invoked by the SMF, ALFs, MSF, or IOFs in the same ensemble, or by a DMF in another ensemble through a peer-to-peer protocol via the TF.

Implementation Considerations. The implementation of a DMF will require a data manipulation language (such as Database Language SQL for data defined by a relational model). Database management systems may provide all the services required of a DMF.

6.2 Transfer Facility (TF)

The Transfer Facility (TF) is the logical entity that interconnects all ensembles. Whereas the other facilities are considered to have a separate manifestation in each ensemble, the TF is considered to be a facility that has one manifestation only, but one that extends across every ensemble. Notwithstanding, that manifestation of the TF in every ensemble has a corresponding implementation in every Component. The logical interconnectivity between two ensembles is thus provided as a result of the functionality of the TF that interconnects the two ensembles. The implementation of the TF in the corresponding Components will result in functionality in each Component together with communications interfaces and one or more communications media between those interfaces.

Network management includes management functions for all layers of open systems interconnection (OSI), naming and addressing, and registration authorities for controlling assignment of names and addresses. Network management will be addressed in part by work being conducted in ISO and CCITT (e.g., ISO 7498-3, *Naming and Addressing*, and ISO 7498-4, *Management Framework*). Those aspects required to ensure interoperability will be addressed by the standards to be adopted for the arc' itecture. These include configuration management and fault management as well as common management information services and protocols.

6.3 Service Control Facility (SCF)

The Service Control Facility (SCF) is the logical entity that binds together all the facilities in an ensemble. The services of the SCF are expected to be provided by the underlying operating system of the implementation. There is no concept of peer interactions between SCFs.

A facility will be explicitly aware of the services that it requires of another facility and will invoke a request for such a service via the SCF. The only standard identified to date that applies to the SCF is the Portable Operating System Interface for Computer Environments (POSIX) (IEEE P1003).

6.4 System Management Facility (SMF)

The SMF is a logical entity intended to provide functionality supplementary to the management services of the DMF and TF for control of parts or all of a system. However, to date, no specific functionality has been identified for SMF that is not provided by DMF and TF. No standards, therefore, have been identified for the SMF. Thus, the system management aspects of Basic Interoperability appear to be satisfied by exchanging system management data and using management services of DMF and TF.

7. Application-Level Facilities

An application-level facility (ALF) is a logical entity that provides services to support the functionality of part or all of one or more Key Tasks. An ALF may be very general purpose, such as a word processor, or may be unique to a single Key Task, such as a battle management decision aid. The entities with which a user interacts, whether directly or indirectly, are ALFs. Some ALFs are therefore likely to contain particular procedures and doctrinal aspects embedded within them that will be specific to an individual nation. These may therefore be more difficult to agree to on a multinational basis and hence will tend, at least initially, to be Nation-specific.

8. Other Facilities

This section describes two facilities that provide additional capabilities over those provided by the four Basic Facilities and the ALFs. They have been specifically identified because they act as interfaces between the architecture on the one hand and users or nonconformant systems on the other hand. Neither of these facilities are required for conformancy, but their use would provide the potential for cost savings.

8.1 MMI Service Facility (MSF)

Users require means to interact with an ADP system. Within the architecture, the MSF has been identified as providing a standard set of user services as the interface between a user and the other facilities within the ensemble. This could be provided separately for every ALF, but providing a unique interface for each ALF would limit flexibility and the potential for cost savings. MSF will provide services both to users, so that they can call on the services of appropriate facilities, and also to those facilities so they can display information to users and solicit responses or input.

8.2 Non-ATCCIS Input/Output Facilities (IOFs)

An IOF is a logical entity for providing the services for interface between conformant systems and nonconformant systems. Because there will be several different nonconformant systems for which interfaces will be required, there will be a family of IOF types rather than a single one. Within an ensemble there can be one of each type of IOF.

One part of the interface between a conformant system and a nonconformant system is not designed in accordance with standards of the architecture. This interface will be an IOF providing the necessary services to pass data out to nonconformant systems and to receive data from those systems.

Standards for IOFs will be defined as required for each type of nonconformant system and will include both data management and data transfer standards. Examples are STANAG 5500 messages.

APPENDIX B

THE USE OF INTEROPERABILITY PARAMETERS TO ENSURE STANDARDS COVERAGE

THE USE OF INTEROPERABILITY PARAMETERS TO ENSURE STANDARDS COVERAGE

1. INTEROPERABILITY PARAMETER METHODOLOGY

1.1 General

This section describes a methodology for ensuring adequate standards coverage through detailed analysis of the parameters that are required to achieve interoperability against specific standards that control these parameters.

1.2 Description of the Methodology

An Interoperability Parameter (IP) is a system or design parameter whose control is required to achieve interoperability. These parameters are identified in system specifications, interface control documents, and other requirements documents prior to or very early in the system development process. In many cases, the interoperability parameters are controlled through the specification of a range of standards. The assembled parameters act as a checklist for interoperability, since each IP must be controlled by a suitable standard. The purpose of an analysis using IPs is to recognize and examine all relevant quantities and characteristics in a direct manner, instead of assuming that existing or draft standards will provide adequate coverage of the quantities.

One of the underlying principles for the ATCCIS concept is that specifying standards is essential to ensuring interoperability. However, it cannot be emphasized too strongly that specifying standards alone will not guarantee interoperability. Indeed, every standard has a number of design parameters or IPs whose values may need to be fixed in the design phase of implementation. To ensure interoperability, each of these IPs must also be specified and controlled. Some IPs are very general and may be used to specify a class of options or mode of operation. Other IPs may be very detailed, such as restrictions on timing, format size, or bandwidth.

IPs can be identified and appropriately controlled in any stage of system development, from initial concepts and requirements to detailed design and as-built specifications. Parameters may simply be the identity of governing specifications (e.g., standards) for interface or other requirements. They could be the identity of options or specification of limits on performance requirements. They could include lists of services or routines that are mandated or that are denied for use. IPs may include logical or physical layouts that show such elements as sequences, relationships, interconnections, and logical block diagrams. IPs may include waveforms. They may include operating procedures, such as dial settings. In short, IPs include any information item that needs to be controlled at any stage of development to ensure interoperability.

Because each standard is a reflection of the degree to which agreement can be reached in a service area, many important attributes (i.e., IPs) are often left unspecified or unaddressed. As agreements are reached over time, the standards will improve by addressing more functionality and harmonizing conflicting approaches. In cases where standards identify extensions and other types of options, great care must be taken in standards specification and IP control to ensure that, whenever an extension or option is permitted, every implementation of the related service also supports this extension or option. This principle is especially important in achieving not only interoperability but also portability of applications from one implementation or environment to another, such as is needed when operating systems, data management systems, interface packages, and hardware are upgraded.

1.3 Examples of Interoperability Parameters

This section provides a brief introduction to interoperability parameters by examining portions of three sets of standards:

- Physical standards for 25-pin connectors (i.e., EIA RS-232D interface)
- Electrical characteristics of digital interface circuits (i.e., EIA RS-423A and QSTAG 594)
- Transmission characteristics for single channel radio (i.e., STANAG 4202).

1.3.1 Physical Standards for 25-pin Connectors

Table B-1 identifies a number of electrical and mechanical interoperability parameters controlled by EIA RS-232D for 25-pin connectors. The first two columns provide the definition of the interoperability parameter; the values specified in the standard, if any, are given in the third column.

Table B-1. Example Interoperability Parameters Based on Characteristics of Unbalanced Load Digital Interface Circuits, 25-Pin Interface Connectors

Description of Interoperability Parameter		Example Value of IP
EXAMPLE ELECTRICAL CHARACTERISTICS:		
Undefined condition	Minimum voltage Maximum voltage	-3 volts +3 volts
Marking condition (binary ONE)	Interface Voltage Maximum	-3 volts
Spacing condition (binary ZERO)	Interface Voltage Minimum	+3 volts
Restriction on use of hysteresis techniques to enhance noise immunity		None
Load impedance of the receiver side	Minimum for applied voltage ≤ 25 volts Maximum for applied voltage of 3 to 25 volts	3,000 ohms 7,000 ohms
Effective shunt capacitance of receiver	Maximum	2,500 picofarads
EXAMPLE MECHANICAL CHARACTERISTICS:		
Number of Pins		25
Cable length	Maximum	Not specified
Connector length (male contacts, female shell)	Minimum Maximum	38.84 mm 39.09 mm
Connector width (male contacts, female shell)	Minimum Maximum	8.23 mm 8.48 mm
Contact spacing, Pin #1	Longitudinal offset Lateral offset	+16.56 mm +1.42 mm
Contact spacing, Pin #2	Longitudinal offset Lateral offset	+15.19 mm -1.42 mm
Contact spacing, Pin #25	Longitudinal offset Lateral offset	-16.56 mm +1.42 mm

Table B-1. (Continued)

Description of Interoperability Parameter		Example Value of IP
Pin diameter	Minimum	0.98 mm
	Maximum	1.06 mm
Pin length, overall with mounting	Minimum	9.77 mm
	Maximum	10.03 mm
Pin mounting length	Minimum	1.57 mm
	Maximum	1.76 mm
Female contact length, overall with mounting	Minimum	9.27 mm
	Maximum	9.63 mm
Female contact socket depth	Minimum	7.37 mm
	Maximum	7.37 mm
Pin assignment	Pin #1	Shield
	Pin #2	Transmitted Data (BA)
	Pin #5	Clear to Send (CA)
	Pin #25	Test Mode (TM)
Female contact socket depth	Minimum	7.37 mm
	Maximum	7.37 mm

Sources:

(1) DIS 2110, *25-Pin DTE/DCE Interface Connector and Pin Assignments* (related to EIA RS-232C), November 1985.

(2) EIA RS-232D, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, 1986.

(3) EIA RS-449, *General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*, November 1977.

(4) EIA Industrial Electronics Bulletin IEB-12, *Application Notes on Interconnection Between Interface Circuits Using RS-449 and RS-232C*, November 1977.

1.3.2 Electrical Characteristics of Digital Interface Circuits

Table B-2 identifies interoperability parameters of digital interface circuits that are controlled by QSTAG 594. These are all electrical characteristics.

Table B-2. Example Interoperability Parameters Based on Electrical Characteristics of Unbalanced Load Digital Interface Circuits

Description of Interoperability Parameter		Example Value of IP
Open circuit voltage, generator	Minimum magnitude Maximum magnitude	4 volts 6 volts
Test termination voltage, generator	450 ohm ±1% test load min	90% magnitude of open circuit voltage
Short circuit current, generator	Maximum magnitude	150 mA
Output leakage current, current, generator	Maximum magnitude with applied voltage from -6 V to +6 V	100 μA
Output signal waveform voltage	Minimum magnitude Maximum magnitude Variance between transitions	3.6 volts 6 volts Within 10% steady state
Output signal waveshaping	Rise time to 90% steady state at maximum signaling rate Minimum Maximum Rise time to 90% steady state at signaling rates below 1 kb/s Minimum Maximum	 0.1 unit interval 0.3 unit interval 100 μsec 300 μsec
High impedance state	Requirement Output voltage at high imped and 450 ohm ±1% test load	Optional Zero (nominal)
Wire or cable	Characteristics	Not addressed
Signaling rates		Not specified
Total load	Resistance minimum Required differential input voltage to achieve intended binary state	400 ohms 200 mV
Fail safe	Requirement	Optional

Sources:

(1) QSTAG 594, *Electrical Characteristics of Digital Interface Circuits*, 25 March 1981 (adopts MIL-STD-188-114).

(2) MIL-STD-188-114A, *Electrical Characteristics of Digital Interface Circuits*, 30 September 1985 (Revision of MIL-STD-188-114 dated 24 March 1976).

(3) ITU-TS V.10/X.26, *Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use With Integrated Circuit Equipment in the Field of Data Communications*, 1985 (related to EIA RS-423A, which is compatible with MIL-STD-188-114A).

(4) EIA RS-423A, *Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits*, December 1978.

1.3.3 Transmission Characteristics for Single Channel Radio

Table B-3 presents a nearly complete summary of the interoperability parameters controlled by STANAG 4202 for single channel radios. This standard is in use in NATO as the basis of interoperability for digital data transmission on combat net radio.

Table B-3. Example Interoperability Parameters Based on Single Channel Radio Standards (STANAG 4202)

Description of Interoperability Parameter		Example Value of IP
Frequency band	Minimum frequency	Not specified
	Maximum frequency	Not specified
	Channel spacing	Not specified
Transmission rates (1)	Preferred rate	600 b/s
	Other required rates	300, 1,200 (and 150 for HF)
Modulation	Type	FSK
Data	Character coding type	NATO 7-bit
FSK modulation	Mark (or 1) frequency	1575 Hz
	Space (or 0) frequency	2425 Hz
	Audio tone frequency accuracy, transmit	± 5 Hz (± 1 Hz desired)
	Receiver accuracy	± 20 Hz
FSK transition between mark & space	Maximum phase discontinuity	5 degrees
FSK timing	Minimum clock accuracy for synchronous data	± 1 part in 10**5
Keytime delay	Required	0.53333, 2.026676 sec
	Options	Multiples of 0.10667 sec (2)
	Modulation applied	Reversals ending in a zero
Bit synchronization preamble	Length	33 bits
	Modulation	Reversals ending in a "1"
Character synchronization preamble	Length	63 bits
	Modulation	Pseudo-random sequence generated by a (6,1) shift register starting with "111111"
Message preparation for transmission	Initial character	"SI" or "NUL" (clear, respectively, encrypted text follows)
	Message structure	7-bit bytes
	Message padding	Up to 6 "1" bits
Cyclic redundancy check (applied to the entire input message)	CRC type	Polynomial
	Generator (mod 2)	x**16+x**12+x**5+1
	Conversion to 8-bit byte	0 in most significant bit
	Size of check	Three 7-bit bytes
	CRC padding	NATO 7-bit end-of-text chars as required (up to 15) (3)
Envelope termination	Size	Four 7-bit characters NATO 7-bit end-of-text chars

Notes:

(1) STANAG 4202 (Appendix B) provides guidelines for interim use of 16,000 b/s channels that are not shown in this table.

(2) 0.10667 sec is the time to send 128 bits at 1,200 b/s or 64 bits at 600 b/s.

(3) The minimum message is 16x7 or 112 bits and requires 0.19 sec at 600 b/s.

Table B-3. (Continued)

Description of Interoperability Parameter		Example Value of IP
Error detection and correction coding (applied to 7-bit bytes)	ED&C type	Hamming (12,7), produces 12-bit coding for every 7-bit byte
Time dispersal coding	TDC interleaving array size	16x12, with sixteen 12-bit Hamming codes
Errors	Number of acceptable but uncorrectable errors	None (stop processing and send no NACK)

Source: STANAG 4202 EL (Edition 2), *Transmission Envelope Characteristics for High Reliability Data Exchange Between Land Tactical Data Processing Equipment Over Single Channel Radio Links*, Military Agency for Standardization, NATO, 25 May 1988.

1.3.3 Interoperability Parameters for X.25 Packet Switching

Table B-4 provides the interoperability parameters for the Implementor's Agreements on the X.25 packet switching protocol as defined in the 1989 NIST Workshop stable agreements that apply to U.S. GOSIP Version 1.0.[1] The NIST Workshop understands that agreement to these interoperability parameters will ensure interoperability of implementations of the X.25 protocols.[2]

2. USING INTEROPERABILITY PARAMETERS TO CHARACTERIZE MILITARY FEATURES IN OSI-RELATED TACTICAL STANDARDS

This section is intended to be expanded to demonstrate the use of interoperability parameters to describe how some fielded tactical data systems are implementing military versions of OSI standards to achieve interoperability. The descriptions here extend the tables provided in Chapter 18 to describe the Quadrilateral Interoperability Program and STAMINA. Examples will also be taken from Appendix C, National Initiatives for Military Use of OSI Standards.

1 *Stable Implementation Agreements for Open Systems Interconnection Protocols*, Version 2, Edition 1, NIST Special Publication 500-16, National Institute of Standards and Technology, December 1988, UNCLASSIFIED.

2 Private communication with Director, Systems and Network Architecture Division, NIST, 25 May 1989.

Table B-4. Interoperability Parameters for X.25 Packet Switching

ISO Layer & Function		Standards Cited	Notes on Interoperability Parameters
-	General	CCITT X.25	• Defines procedures required to describe the DTE side of a CTE/DCE interface for systems attached to subnetworks providing an X.25 interface shall be as defined in ISO 7776 and ISO 8208 as indicated below. • These procedures shall also apply to a DTE operating on a DTE/DTE interface.
3	Network Layer	ISO 8208 (X.25 PLP)	• The elements of ISO 8208 applicable for use depend on the OSI role of ISO 8208 (i.e., provision of CONS, support of CLNP): a. When ISO 8208 is used to support CONS, the optional user facilities in Section 5.1 of ISO 8878 shall be supported. b. When ISO 8208 is used to support CLNP (when providing the CLNS), Permanent Virtual Circuit may be used. • Virtual Call Service is required. • Any mutually agreed window and packet size may be used; however, all DTEs must be capable of supporting a window size of 2, a packet size of 128 octets, and a sequence number modulus of 8. • The Basic RPOA Selection Facility shall be implemented and its use or non-use selectable on a per virtual call basis. (1)
2	Data Link Layer	ISO 7776 (HDLC Procedures-- X.25 LAPB)	• The address assignments are: DTE = A (=11000000 binary) DCE = B (=10000000 binary). On a DTE/DTE interface, one of the DTEs, by a prior agreement, shall use the DCE address. • The modulus shall be 8. • A window size (k) of 7 shall be supported. In addition, other window sizes may also be supported. • The Multilink Procedures are excluded.

Notes:

1. Agreement on the Basic RPOA Selection Facility parameter is an ongoing, not a stable, implementation agreement.

References:

1. *Stable Implementation Agreements for Open Systems Interconnection Protocols*, Version 1, Edition 1, NIST, December 1988.
2. *Ongoing Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements*, NISTIR 88-3824-2, NIST, February 1989.

(This page intentionally left blank)

APPENDIX C

NATIONAL INITIATIVES FOR MILITARY USE OF OSI STANDARDS

NATIONAL INITIATIVES FOR MILITARY USE OF OSI STANDARDS[1]

1. INTRODUCTION

This appendix identifies profiles being used in national initiatives that make or plan to make significant use of OSI standards in military applications. The purpose is to provide detailed information on profiles that are planned for evolving tactical CCISs in the nations. Additional contributions to this appendix (as well as other parts of this document) are welcome.

NATO work on OSI is discussed in Chapter 17. Major bilateral and multilateral NATO initiatives are discussed in Chapter 18; these include the Quadrilateral Interoperability Program and STAMINA. Many national initiatives are discussed in Chapter 19.

2. CCIS PROFILES FOR INTEROPERABILITY

2.1 Details of Standards for French National Initiatives for Enhanced Interoperability

The Army will use standardized products based on the following standards:

- Programming language: LTR3 (Language Temps Reel), Ada, C
- Database: Relational database management systems, SQL
- Operating System: UNIX
- Development methods: Based on the French military standard GAM-T-17.

2.2 Overview of Data Communications for US Army's ATCCS

The Army Tactical Command Control System (ATCCS) architecture is discussed in Chapter 19 (Section 19.1.6). This section highlights the organization of data communications services planned for ATCCS.

Figure C-1 identifies the protocol stacks specified in the Initial Baseline, and Figure C-2 identifies the protocols for the next stage [termed "Effectivity A1.1" and planned for the Follow-On Test and Evaluation (FOT&E) milestones] for ATCCS.[2]

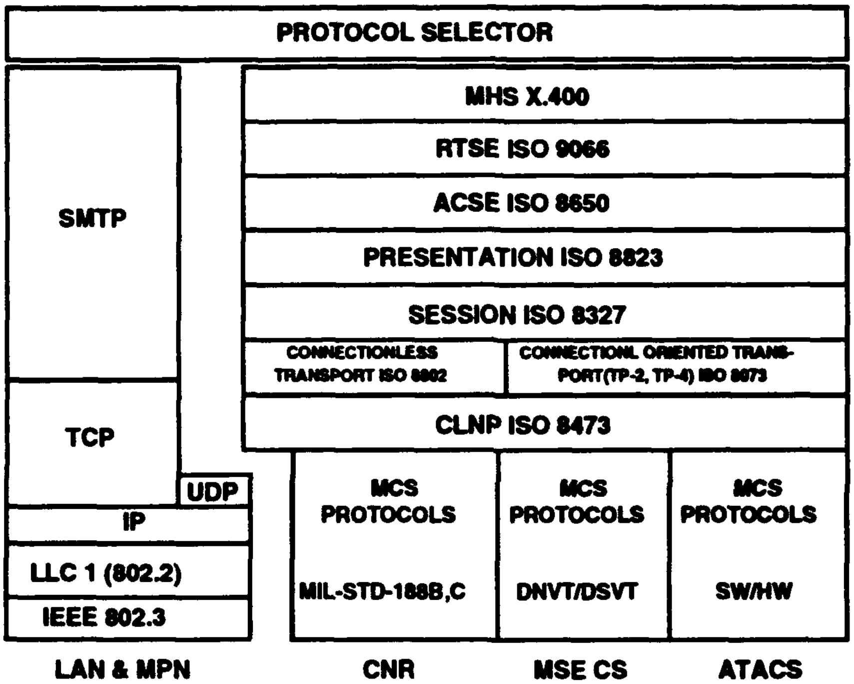
- The local area network (LAN) interface is defined by TCP/IP, IEEE 802.2 (LLC 1) and IEEE 802.3 (CSMA/CD).
- The MSE Packet Network (MPN) uses TCP/IP, ITU-TS X.25, HDLC LAPB (ISO 7776) and four-wire conditioned diphase (CDP) or fiber-optic Thin LAN.
- US DoD Internet protocols used over TCP/IP are File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), and TELENET. The standards for those protocols are listed in Appendix H.
- The UDP is provided to permit stacks over the Connectionless Network Protocol (CLNP) to use the MPN and LAN communications.
- Combat Net Radio (CNR) interfaces are defi d by MIL-STD-188 B and C, STANAG 4202, and MIL-STD-188-114A.
- The ATCSS Common Hardware/Software (CHS) will provide protocols at Layers 2, 3, and 4 (in part).
- The MSE Circuit Switch (CS) interface is through the Digital Non-Secure Telephone (DNVT) and Digital Secure Telephone (DSVT).
- The CHS provides physical interfaces to the Army Tactical Communications System (ATACS).

---

1 Effective date of this Appendix is January 1992.

2 Cross-Functional Area Interface Specification for ATCCS, ACCS-A3-400-12, U.S. Army CECOM.

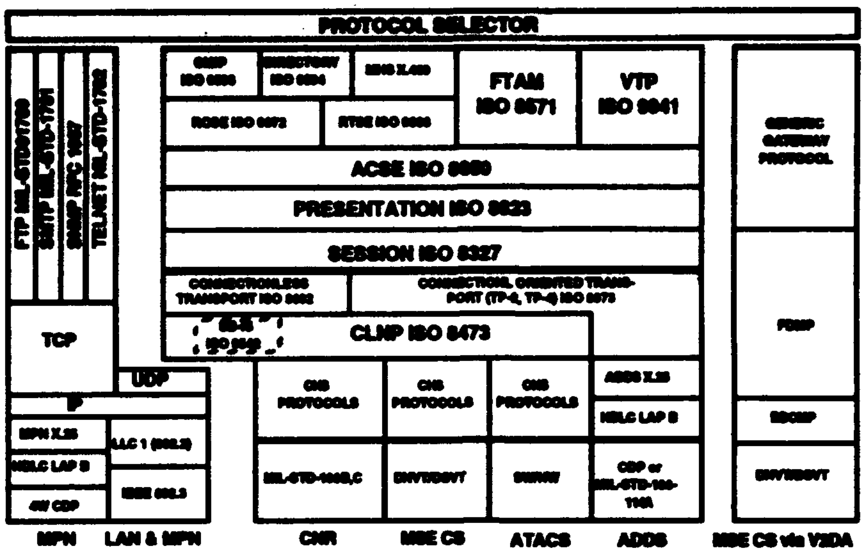
- Except for the Air Defense Functional Area, which also uses the Joint Tactical Information Distribution System, the ATCCS users will use only the Enhanced Portion Location Reporting System (EPLRS) portions of the Army Data Distribution System (ADDS). EPLRS uses a CDP or MIL-STD-188-114A interface, HDLC Lap B, and an ADDS version of X.25.[3]
- An alternate MSE CS Generic Gateway is provided by use of the DNVT/DSVT, DD CMP and (Full Duplex Message Protocol (FDMP). This uses the MSE Version 2 Data Adapter (V2DA), currently only in use by the All Source Analysis System (ASAS).
- Not shown is the optional use of BLACKER with the MPN stack.
- Not shown is the Quadrilateral stack use with MCS (see Chapter 18). This stack uses TP2 and a variant of MHS-84.
- Not shown are options for LAN and MPN to use an address resolution protocol (ARP) and a reverse address resolution protocol (RARP).



Source: Cross-Functional Area Interface Specification for ATCCS, ACCS-A3-400-12, U.S. Army CECOM.

Figure C-1. ATCCS Inter-BFA Communications Protocols (Initial Baseline)

3 ADDS X.25 and MPN X.25 are not identical and not reported to be interoperable.



Source: Cross-Functional Area Interface Specification for ATCCS, ACCS-A3-400-12, U.S. Army CECOM.

Figure C-2. ATCCS Inter-BFA Communications Protocols (Effectivity)

2.3 Advanced Field Artillery Tactical Data Systems (AFATDS)[4]

AFATDS is the Fire Support (FS) functional area control system of the Army Command and Control System (ACCS) and Marine Tactical Command and Control System (MTACCS).

2.3.1 System Overview

AFATDS will provide an automated command control, and coordination system which satisfies the Fire Support requirements generated by AirLand Battle doctrine. AFATDS equipment will be employed worldwide in support of the U.S. Army Fire Support Battlefield Functional Area (BFA) and Marine Corps fire support requirements. AFATDS software development will be accomplished in successive versions, each implementing additional functionality and interfaces, beginning with Version 1; Versions 2 and 3 will expand AFATDS functionality through development on its predecessor version.

AFATDS Version 1 will include component elements provided by the Army Tactical Command and Control System Common Hardware and Software (ATCCS CHS) program and the Standard Integrated Command Post System (SICPS) program.

AFATDS is a multi-service United States Army/United States Marine Corps (USA/USMC) automated command and control (C2) system for Fire Support Operations (FSOP). The initial fielding of AFATDS will be Version 1 (V1), which will be capable of managing field artillery (FA), air fire support (AFS)/Marine Air naval gunfire (NGF) and mortar attack systems at all echelons from corps to platoon level. AFATDS will provide the capabilities to process, analyze, and exchange combat information within the AFATDS architecture and with other Army BFA systems, selected NATO systems, and Marine Tactical Command and Control System (MTACCS) component systems in Marine Amphibious Air-Ground Task Forces (MAGTFs).

AFATDS will be a system of mobile, dispersed, multi-functional nodes providing automated planning and execution capabilities to fire support operational facilities (OPFACs) and Independent User Centers (IUCs). OPFACs will operate at Fire Support Elements (FSEs) of the supported maneuver force, field artillery command posts, and other FA elements throughout the command structure. IUCs are remote terminals that allow commanders and selected fire support personnel to monitor fire support operations and issue guidance and directives from widely dispersed battlefield locations. The operational context for AFATDS is given for the Army in Figure C-3 and for the Marine Corps in Figure C-4.

---

4 This section is based on the following contribution: AFATDS Data Communications, Draft, Henry Saphrow, OPM AFATDS, U.S. Army CECOM, January 1992, UNCLASSIFIED.

The AFATDS V1 contract was awarded in May 1990 with IOT&E planned for FY94. AFATDS V2 and V3 are parallel efforts starting in FY92 for Version 2 and FY94 for Version 3. Initial fielding of production version (V2) is planned for FY95.

2.3.2 FS Operational Capabilities

AFATDS OPFAC capabilities within FA units will be for the command, control, and support of organic and attached FA assets (i.e., target acquisition means, operation centers, fire direction centers, weapons, and FA mission support elements). OPFAC capabilities located with maneuver units (FSE) will support the advising of the maneuver force commander on the use of available fire support assets, planning their employment, and integrating them into the scheme of maneuver. Marine Corps requirements are identified in the FIREFLEX Required Operational Capability. Automated capabilities will also be provided within any designated OPFAC for performing the fire support execution and movement control functions.

AFATDS FS operational capabilities are contained in five general operational need categories. These categories are the following:

a. Fire Support Planning (FSP) - provides the overall planning capabilities for integration of field artillery, air fire support, naval gunfire, and mortars into the force's scheme of maneuver.

b. Fire Support Execution (FSX) - provides automated support for target processing, attack systems analysis, and tactical fire direction.

c. Movement Control (MC) - provides for the movement control of field artillery units, prepares movement requests, coordinates those requests with the appropriate force level headquarters, and maintains movement data.

d. Field Artillery Mission Support (FAMS) - provides for logistical support for the field artillery system.

e. Field Artillery Fire Direction Operations (FAFDOPS) - maintains the current status of fire missions, fire support and field artillery units.

2.3.3 Interoperability Capabilities

AFATDS will interoperate with existing tactical systems in order to serve as an integral element in the overall command and control structure. These systems consist of those FS systems directly engaged in execution of the Field Artillery mission and those other control systems which form the ATCCS. The following list summarizes the principal Version 1 AFATDS interfaces.

a. FS Sensor Systems (e.g., Firefinder, DMD, DCT, ATHS)

b. FS Weapons Control Systems (e.g., BCS, MBC, FDS)

c. Adjacent Systems [e.g., TACFIRE, ADLER, LTACFIRE, AFATDS (USMC)]

d. Maneuver Control System (MCS) - BFA and Force Level Control (FLC)

e. All Source Analysis System TOC Support Element (ASAS TSE) - Intelligence/ Electronic Warfare (I/EW) Data

f. Forward Area Air Defense Command and Control (FAAD C2) - Air Defense Support

g. Met Data System - Technical fire control meteorological data

h. AFATDS Operators.

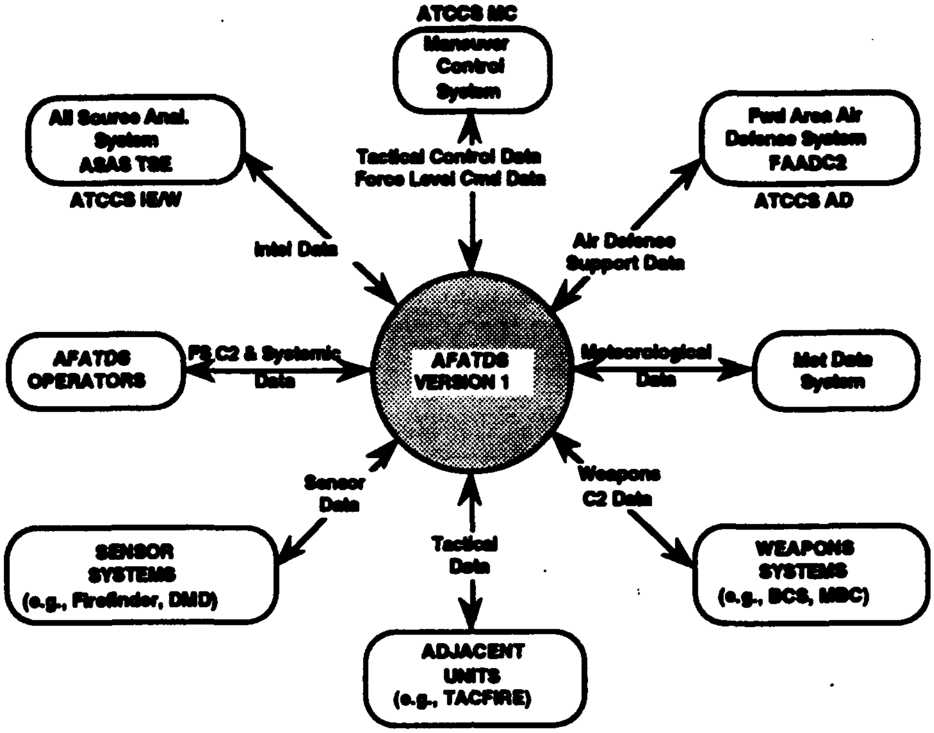


Figure C-3. AFATDS (US Army) Operational Context

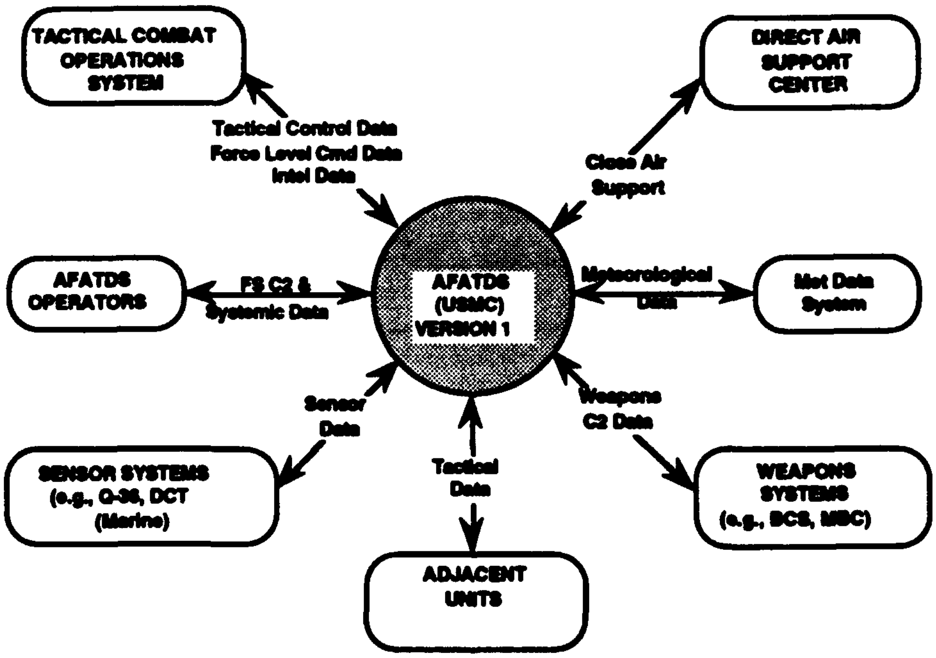


Figure C-4. AFATDS (USMC) Operational Context

Note: AFATDS will be a system of mobile, dispersed, multi-functional nodes providing automated planning and execution capabilities to fire support operational facilities.

2.3.4 AFATDS Communication Requirement

AFATDS primary method of communication is via the Combat Net Radio (CNR). Other communication capabilities includes Area Common User System (TRI-TAC, Mobile Subscriber Equipment, and Unit Level Switch), Army Data Distribution System (ADDS) and Position Location and Reporting System (PLRS), field wire (2W, 4W) and local area network (IEEE-802.3). AFATDS communication requirements include: operation on the move, continuity of operations (CONOPS), alternate net routing, communication channel reconfigurability while system is operational, operation with four programmable communication channels, receive, transmit, and process over 2,000 messages per hour over secure link. Additional requirements include: detection reduction by the enemy, multiple destination communication, network loading and balancing, and automatic relays. To meet heavy traffic demand and reliable communication over the CNR, AFATDS design implemented a communications architecture described in the next section.

2.3.5 AFATDS Communications Architecture

Figures C-5 and C-6 illustrates the organization of communications protocols used between FSWs with regard to the ISO OSI Basic Reference Model, ISO 7498. Applications processes utilized one or more Application Service Elements (ASEs) which embody the functions of the ISO/OSI model's application, presentation, and session layers. Examples of ASEs are file transfer, message exchange, and X-Windows. ASEs rely on the data transfer services of transport and lower layer protocols that are common to all Fire Support Workstations (FSWs), to facilitate their peer relationships.

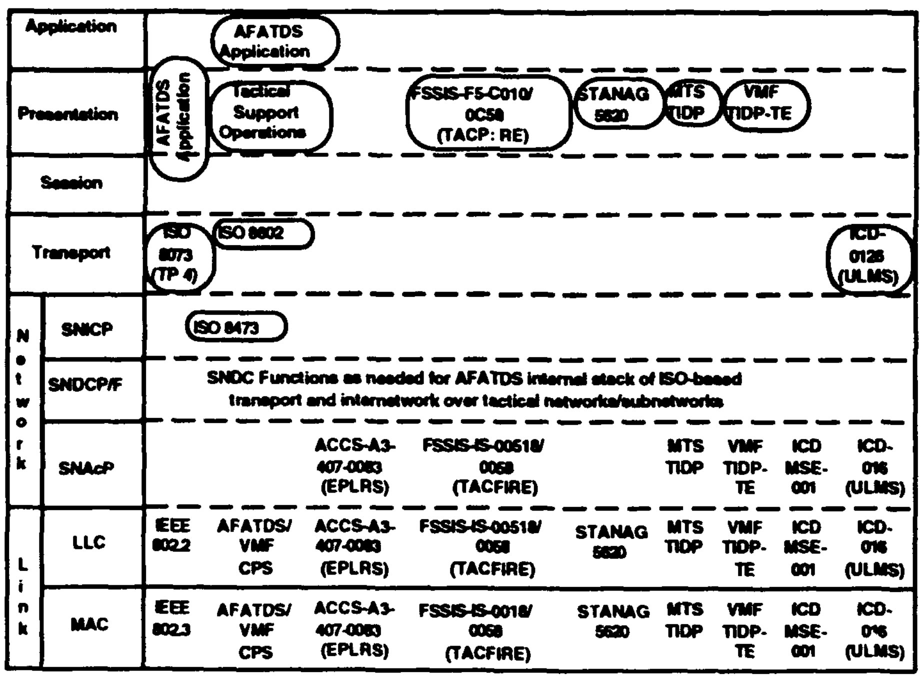


Figure C-5. Organization of Communications Protocols in AFATDS

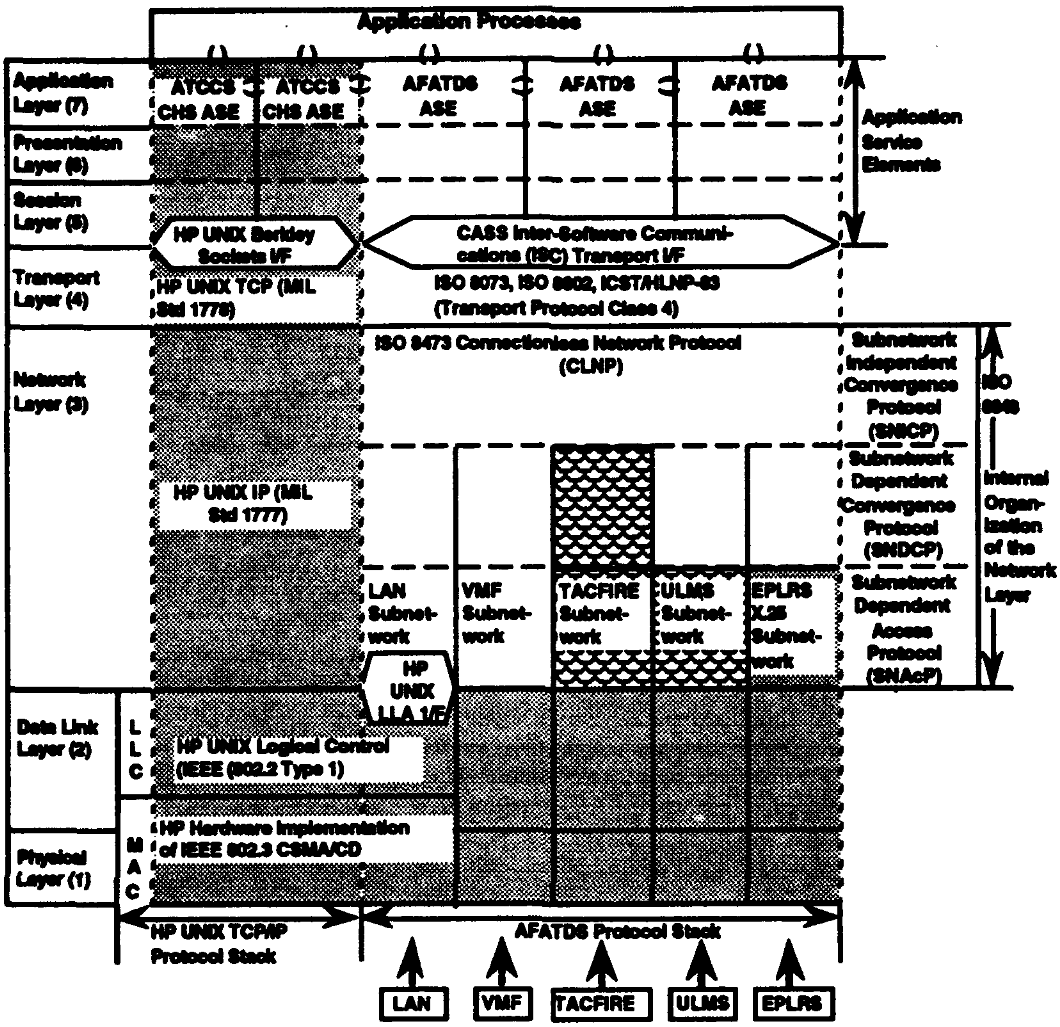


Figure C-6. AFATDS Protocol Stacks

Physical Layer. Connections to the following devices are provided in the Physical Layer.

- UHF: SINCGARS Radio, VRC-12, AN/PRC-77, AN/PRC-68
- HF: AN/PRC-104, AN/GLC-213, AN/GRC-193, AN/GRC-106
- MSE: DNVT, DSVT, EPLRS, PLRS, and ULS.

Data Link Layer. The data link is based upon Joint VMF-TIDP-TE Vol IV. Presently this standard only supports Type I services. AFATDS/VMF CPS (AFATDS Variable Message Format Communications Protocol Standard) supports both Type I and Type II services. Type I is based on MTS Broadcast standard with enhancements agreed by the Joint Message Standard Working Group. The Type II services are based on IEEE 802.2 and HDLC Lap B protocols with some enhancements for Combat Net Radio (CNR). The following enhancements are part of AFATDS/VMF CPS:

- Multi-Frame Transmissions
- Uncoupled Acknowledgements
- Use of Poll/Final (P/F) Bit
- Implementation of "Windowing" for Multi-Frame Transmissions
- Use of Sequence numbers for State Variables
- Selective Rejection Balanced Mode Extended (SABME) Frame
- Frame Reject (FRMR) Frame

- Reset (RSET) Frame
- Disconnect (DISC) Frame.

Network Layer. The following network layer functions, which have been derived from the AFATDS SSS requirements and CEP experience, will be supported for AFATDS Version 1.

- Interconnection of Subnetworks
- Addressing
- Routing
- Error Control
- Flow Control
- Subnetwork Independent Convergence Protocols (SNICPs)
- Subnetwork Dependent Convergence Protocols (SNDCPs)
- Subnetwork Access Protocols (SNAcPs).

The network layer implementation for AFATDS will be based on the DIS 8473 (CLNP), ISO 8648, ISO 8348, and ISO 8348/ADD 1 network layer standards. Due to the unique FS requirements and the FS operational environment, these standards will be extended and modified as necessary for AFATDS use. The AFATDS CLNP-based internet protocol will be utilized as the SNICP over five distinct subnetworks: the LAN provided as part of the ATCCS CHS, tactical networks employing the VMF-TIDP-TE data link protocol, tactical networks employing TACFIRE protocols, Enhanced Position Location Reporting System (EPLRS) X.25-based networks, and Unit Level Message Switch (ULMS)-based networks.

ISO 8473: Information processing systems - Data Communications - Protocol for providing the connectionless-mode network service. This is the standard that AFATDS has adopted in which to base the internetwork layer. The AFATDS CLNP functionality will use multiple SNDCPs to access the diverse suite of subnetworks available to it and required of it to gain the connectivity needed in the Army's limited channel/bandwidth environment. Currently, the inactive Network Layer protocol subset will not be used even within an OPFAC LAN in order to support the dynamic (re)configuration capability required in AFATDS. The Non-Segmenting protocol subset may-or may not be utilized awaiting results from yet-to-come performance trade-offs. Given the multiplicity of subnets with their varying packet sizes, a segmenting capability would seem appropriate in an absence of realizing the reliability of the subject subnets.

Session Layer. The Session Layer is null for AFATDS data communications.

Transport Layer. The following Transport Layer functions, which have been derived from the AFATDS System/Segment Specification (SSS) requirements and Concept Evaluation Phase (CEP) experience, will be supported for AFATDS Version 1.

- Connected Data Transfer
- Acknowledged Unit Data Transfer
- Unacknowledged Unit Data Transfer
- End To End Acknowledgement
- Retransmission on Time Out
- Segmenting and Reassembly
- Data Sequencing/Resequencing
- Explicit Flow Control
- Transport Addressing
- Inactivity Control.

The transport layer implementation for AFATDS will be based on ISO 8073 (TP 4), ISO 8072, ISO 8072/DAD 1, ISO 8602, and ICST/HLNP-83 transport layer standards. Due to the unique Fire Support requirements and the FS operational environment, these standards will be extended and modified as necessary for AFATDS use.

ISO 8073: Information processing systems - Open System Interconnection - Connection Oriented transport protocol specification; also ISO 8073/DAD 2: Addendum 2: Operation of Class 4 over Connectionless Network Service. These are the standards which AFATDS has adopted to base the transport mechanism on. AFATDS CEP developed a transport mechanism based on NIST recommendations for implementing TP4 as promulgated in ICST/HLMP-83-3: Proposed FIPS - Specification of a Transport Protocol for Computer communication, vol. 3: Class 4 Protocol. The primary extension to TP4 adopted from the NIST document was the

modification of UNIT_DATA from unacknowledged/unreliable to acknowledge/reliable. This extension was developed by NIST to support military application and coincidentally served AFATDS CEP well. Additionally specializations to the TP4 protocol were made in CEP to meet the requirements of its clients and the diverse nature of the subnetworks (IEEE 802.5 to CNR) it was used over. Timer durations were modified to account for service delays perceived on different nets and to account for non-responsiveness of clients in reacting to service indications (e.g., connection offers). An adaptive retransmission timeout mechanism was developed. Segment sizes were adjusted per the servicing networks ability (non-segmenting network used in CEP). New state transitions and protocol data units were introduced to account for AFATDS specific anomalies or needed utilization improvements. An example was the inclusion of large amounts of user data in CR TPDUs in FIPS type UNIT_DATA to limit the number of TPDUs required to complete an acknowledged "datagram" especially over CNR. This AFATDS CEP implementation of a transport layer (in Ada) has been ported to AFATDS V1 for use as a protocol communication system in support of the AFATDS Inter-Software Communication (ISC) prototype, and portions will be used where possible in the AFATDS V1 objective system design and implementation.

ISO 8062: Information processing systems - Open System Interconnection - Protocol for providing the connectionless-mode transport service. Despite having needed and adopted NIST FIPS-style acknowledged UNIT_DATA, AFATDS still intends on availing itself of the more original ISO unacknowledge UNIT_DATA mechanism. This is useful especially in support of multicast. In AFATDS CEP this same standard was adopted (in draft form) and mechanisms were developed to allow multiple endpoints, or TSAPs, within a single workstation to receive copies of a single, multi-cast on the LAN.

Presentation Layer. The Presentation Layer is handled by the Tactical Support Operation (TSO) function in AFATDS. The TSO is a computer software configuration item (CSCI) in AFATDS V1 that embodies the presentation functions necessary to afford AFATDS applications the ability to interoperate with multiple different end systems many of which have different transfer syntaxes (i.e., message formats/sets). TSO acts as a translation filter on transmission from AFATDS applications, proper, which can be destined to AFATDS and non-AFATDS systems alike, and proxies the transmission request on the correct procedural interface: Inter-software communication (ISC) for intra-AFATDS transfer or the appropriate external system (XC) interface for non-AFATDS transfers. In the intra-AFATDS case, the ISC delivers the transmission to the destination application software entity directly, which receives it via TSO proxy routines again. In the non-AFATDS case, TSO invokes the XC function which RPCs (remote procedure call) the transmission request via the ISC to its agent XC entity at the respective external system "communication gateway" entity, which in turn acts as a gateway between the AFATDS internal stack, accessed via ISC, and the external stack required to interact with the non-AFATDS system.

TSO fills the classical role of application gateway as well. On reception of a message transmission from an external system, the appropriate "communications gateway" entity passes the message off to TSO, which then translates the message to AFATDS internal format and forward it on to the application entity within the OPFAC which must process it. This hand-off on reception is done because external systems do not address their transmissions to the level of granularity that the AFATDS does. In essence, the other systems utilize a one-level address space where addressing consists of identifying the fire support unit. However, AFATDS utilizes a two-level name-space where each intra-AFATDS transmission is addressed not only to the unit, but also to the specific software entity within the unit, which by the way may be configured to be anywhere within a multi-workstation OPFAC. This is because AFATDS is the first distributed system in the US fire support inventory coupled with the engineering capability to extend transport end-to-end reliability over internetted tactical networks, whereas in the past it was all done with link protocols. At any rate, TSO is required to determine the final destination based on message content because the data transfer mechanism was not given complete address information by the external system per AFATDS standards.

Application Processes. AFATDS applications processes are composed of ASEs that can be classified into two types: Common ASEs and Specific ASEs. Common ASEs are those that provide capabilities which are generally useful to more than one application process. Specific ASEs are those that provide capabilities to satisfy the particular needs of a single application process. An ASE may invoke the services of another ASE within the same application process. Therefore, Common and Specific ASEs are combined in various ways to create different applications processes. Individual ASEs employ Application, Presentation, and Session Layer functions as necessary based on the service that the ASE is providing. Therefore, it is not possible to identify a single set of application, presentation, and session protocols, but rather these layers must be discussed for each ASE employed by an application process. The specific application processes and ASEs they employ are described below.

Application Layer employs two services. In the classic case, software entities access the data transfer mechanism directly (ISC in AFATDS, Berkley Sockets, or TLI in UNIX) and perform their own version of the required functionality typically associated with the upper layers. In effect, the applications use their own ASE.

This is especially true when remote procedure call (RPC) paradigms are used. RPC is an underpinning of AFATDS given its distributed nature and non-deterministic configurability. In the second service, application level software entities access data transfer by utilizing Message Handler Services defined as Tactical Support Operation (TSO). TSO performs some application control functionality, presentation functionality and to some extent handles sessions with external systems for AFATDS applications. The message definition effort will use the data elements and messages as defined in ACCS, DoD (Joint), and NATO standards.

2.4 Protocols Provided by US Army TCIM Hardware[5]

The US Army Common Hardware/Software (CHS) programs include a Tactical Communications Interface Module (TCIM). Two types of interfaces are provided. Supported by an internal or an external device, Channel 1 supports the Maneuver Control System (MCS) Version 10 Circuit Switch (CSW), the Marine Tactical System (MTS) Mode VII CSW, ITU-TS X.25, and the Army Data Distribution System (ADDS) X.25 for EPLRS. The Version 1 interfaces are:

- KY-68 (DSVT)
- TA-1035 (DNVT)
- KG-84 (DLED)
- AN/GYC-7 Unit Level Message Switch (ULMS)
- SB-3614 SB
- EPUU/JTIDS (32 Kbps)
- 4 Wire
  - FSK-188C&B
  - STANAG 4202 (Annex A)
  - Conditioned Diphase.

The second type of interface is available on both Channel 1 and Channel 2) and is also supported by an internal or exernal SCSI circuit card. The second type supports all the interfaces defined by Version 1, together with additional interfaces noted below, on two channels (Channels 1 and 2). The Version 2 capability supports combat net radio with the following added interfaces:

- Combat Net Radio
  - VRC-12 and PRC-77
  - SINCGARS
  - GRC-193, GRC-213
  - PRC-104
- KY-57
- 2 Wire
  - FSK-188C&B
  - STANAG 4202 (Annex A)
  - Conditioned Diphase.

The following requirements were added as follow-on TCIM requirements for field tests in 1992:

- AFATDS:
  - TACFIRE protocol (6/9/11/8) software
  - NATO STANAG 5620 software
  - MTS switched software
  - ADDS interface software
  - VMF TIDP software
  - TCIM/TCU interface
  - KG-84C

[5] This section is based on the following contribution: *CHS Communications Program*, Briefing, Draft, 'an Levine, OPM CHS, US Army CECOM, December 1991, UNCLASSIFIED; and a private communication with Stan Levine in February 1994 [Ref. Levine 1994c].

- FAADC2I
  - Multiple TCIM
  - ADDS interface
  - TCIM/TCU interface
- ADDS
  - ADDS interface software
    - -- 128 Kbps baud rate
    - -- 200 packages per second (pps) throughput
  - Two programmable PJH channels
  - TCIM/TCU interface
- Marine Corps
  - MTS switched software
  - MTS broad cast (Class I) software
  - ULS autodial interface software
  - KG-84C interface software
- MCS follow-on requirements
- FSAC follow-on requirements.

The overall architecture for the communications software interfaces between the physical device (SCSI Bus) and the Layer 3 services provided by the Unit Level Processor (ULP) is shown in Figure C-7.

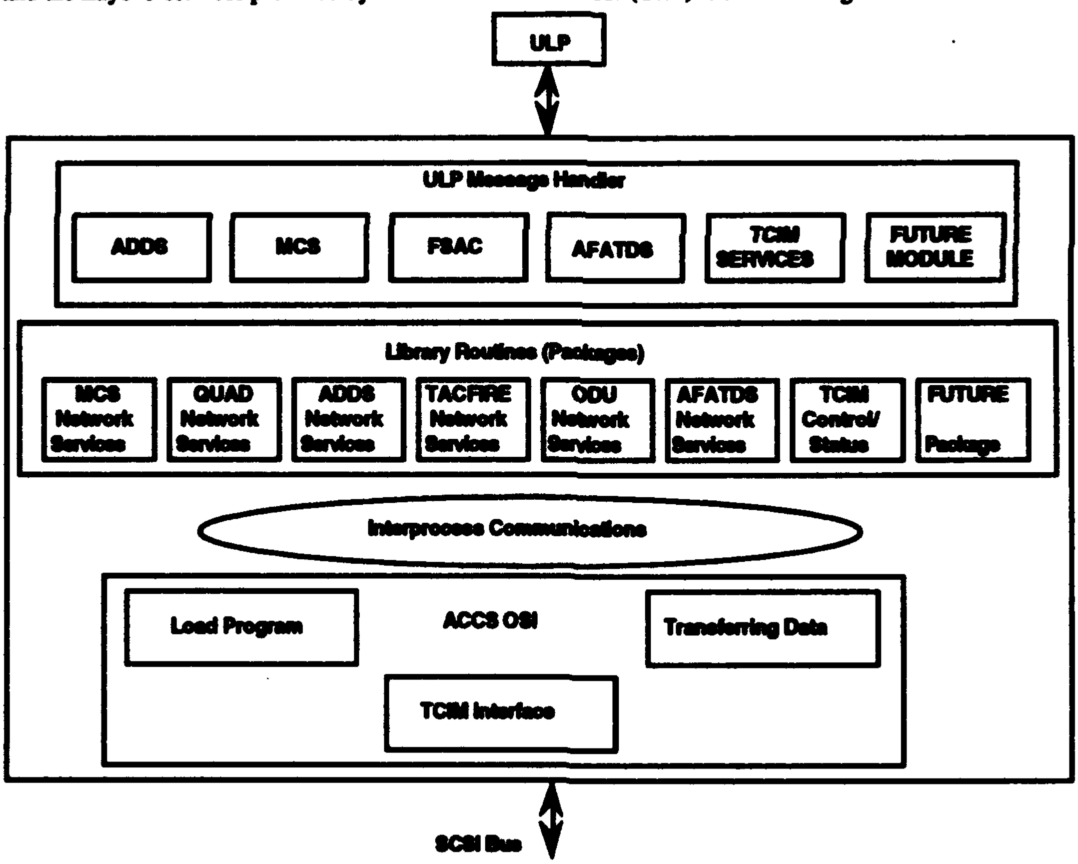


Figure C-7. Communications Software Interface Architecture

3. EXAMPLE PROFILES FOR BROADCAST MEDIA

3.1 Example of a Broadcast Profile for Data Communications Using Tactical Radios

This section uses the OSI Reference Model and interoperability parameters to identify interpretations, extensions, and deviations to OSI and other standards in the specification of a set of protocols used to support data transmission over combat net radio by the U.S Marine Corps. These protocols are specified in Volume V of the Marine Corps MTS TIDP.

The MTS protocols were developed based on U.S. federal standards in the late 1970s. Many of the standards selected have become ISO standards, and the structure of the MTS protocols can be interpreted in terms of the seven-layer OSI Reference Model. The MTS broadcast profile, discussed in this section, is now being used by the Army and the Marine Corps as the basis for defining the initial protocol standards to be used in the TIDP now being developed for Joint Interoperability of Tactical Command and Control Systems (JINTACCS) K-Series Variable Message Format (VMF) bit-oriented messages. The K-Series messages and associated data communications protocols are being specified by the joint Fire Support Subgroup (FSSG) of the Joint Multi-TADIL Standards Working Group (JMSWG) under the auspices of the Joint Tactical C3 Agency.

Table C-1 highlights the features provided in the broadcast protocol, used in Marine Corps tactical data systems (TDSs), for each of the seven layers. It further identifies the standards used in each layer and notes the interpretations, exceptions, extensions, and deviations that were specified.

Military features supported by the broadcast protocol standard and identified in Table C-1 include:

- Multiaddressing (Layer 7, through the Message Header; and Layer 2, through the extended address field)
- Data integrity and, more generally, the capability to operate in a high bit-error-rate environment [Layer 2, through use of a 32-bit frame check sequence (FCS) for error checking and the (23,12) half-rate Golay error detection and correction coding (ED&C), together with 16x24-bit interleaving]
- Use of XID command and response (Layer 2)
- Control of emanations by senders and recipients through provisions for optional acknowledgements (ACKs) (Layer 7--request for ACK is part of the message) and for not sending ACKs even when requested (Layer 2), both under operator control
- Limit on the number of retransmissions permitted (Layer 2)
- Providing for net access (uses an international standard in Layer 2 for handling media access contention and collision detection[6] and defines an algorithm for wait times for reattempting access); net access algorithms could be extended to support precedence and preemption.

4. EXAMPLE PROFILES FOR TACTICAL SWITCHES

4.1 Example of a "Datagram" Switched Protocol Standard for Tactical Radios

This section summarizes a set of protocols used to support data transmission through tactical data switches by the U.S. Marine Corps. These are the MTS switched protocols that are specified in Volume V of the Marine Corps *Technical Interface Design Plan for Marine Tactical Systems*.

Table C-2 highlights the features provided in the switched MTS protocol for each of the seven layers. The table identifies the international and U.S. standards used in each layer, and notes the interpretations, exceptions, extensions, and deviations that are specified.

[6] The listen-before-talk contention method is called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Table C-1. A Functional Profile of Broadcast Protocols Used in Tactical Systems by the U.S. Marine Corps

ISO Layer, Function		Standards Cited	Notes on Interoperability Parameters
7	Msg Header Msg Acknowledgment	None None	Supports multiple addresses, precedence, and security classification.
6	Msg Format	None	Uses the same flagging scheme as the syntax adopted for U.S. JINTACCS K-series messages.
	Information Field Size	None	Maximum message length is 3500 octets.
5	None	N/A	Null layer.
4	None	N/A	Null layer.
3	Message Segmenting	N/A	Messages are not segmented.
2	Frame Formatting	ISO 3309/7809 (HDLC) with Options 7 and 14	Opt 7=Extended Address Field; 2-17 octets (base std is one octet; Opt 7 specifies no maximum on extended address field size). Opt 14=32-bit frame check seq (FCS) (base standard is 16-bit FCS).
	Frame Addressing	ISO 3309	
	Commands & Responses	ISO 4335/7809 with Option 1	Opt 1=XID. Does not support SABM, DISC cmds and FRMR,UA,DM resp (radio application). Does not support P/F bit.
	Media Access	No standard applies	Uses CSMA/CD with unique algorithms for reattempting access to net.
	Data Link Initialization and Release	ISO 4335/7809 with Option 1 (XID)	XID is used during net establishment.
	Frame Transfer	ISO 4335/7809	Uses all 3 types of frames.
	Acknowledgment (ACK)	ISO 4335	ACK is optional; when invoked, it follows the standard.
	Retransmission	Not controlled by standards	Max 2 retries (under operator control) (no provision for setting a max in stds). Standards suggest use of P/F bit to control retransmission.
	ED&C--Error Detection	IS 3309/7809 w Opt 14	32-bit FCS (algorithm is ISO 3309, Sec 3.6.3).
	ED&C--Error Coding	Not controlled by standards	(23,12) half-rate Golay; 24th bit is zero filled (detects 6/corrects 3 errors in each 24-bit codeword).
	ED&C--Interleaving	Not controlled by standards	16x24-bit time dispersive coding (TDC).

Table C-1. (Continued)

ISO Layer, Function		Standards Cited	Notes on Interoperability Parameters
1	--Electrical		
	--Voltage Levels	MIL-STD-188-114	[Similar to CCITT V.10/X.26]
	--Load Impedance	MIL-STD-188C	
		MIL-STD-188/24(Prt2)	
		MIL-STD-188-141	
	Mechanical		
	--Connectors	MIL-STD-242G(Prt8)	
		MIL-P-55149	
	Cable Lengths	MIL-STD-242G(Prt8)	
	Functional (pin assign)	MIL-STD-242G(Prt8)	
	Procedural		
	--COMSEC Pre/Postamble		
	Frame Placement	DCT Spec	
	--Keytime Delay	DCT Spec	
	--Bit Synchronization	DCT Spec	
	--Transmission Synch	DCT Spec	
	--Clocking Ctrl & Timing	N/A	

References:

1. Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP), Volume V, Protocol Standard, Headquarters, U.S.Marine Corps, July 1987, UNCLASSIFIED.
2. Discussions with Systems Integration Directorate, MCRDAC, and LOGICON/Eagle Technology, Inc., March 1989.

Table C-2. A Functional Profile of "Datagram" Switched Protocols Used in Tactical Systems by the U.S. Marine Corps

	ISO Layer, Function	Standards Cited	Notes on Interoperability Parameters
7	Msg Header Msg Acknowledgment	None [1] None	• Supports multiple addresses, precedence, and security classification.
6	Msg Format Information Field Size	None None	• Uses the same flagging scheme as the syntax adopted for US JINTACCS K-Series messages • Max is 40 segments, 260 octets per segment (message length)
5	None	N/A	• Null layer
4	End-End Sequence Control End-End Congestion/ Flow Control	None None found	• Transport layer accumulates and orders packets for users; uses 7 octets (vice 20-60 octets for TCP) • Connectionless-oriented layer, a variant of TP4
3	Network Routing/Switching Message Segmenting Packet Addressing Packet Precedence Network FLow & End-End Error Recovery (Message Accountability) Congestion Control Internetting	None found Not controlled by standards None None None found None N/A	• Connectionless-oriented with deterministic routing [2] • Supports "floating" host, using operator-initiated disconnect and reconnect, but requiring no change of address • 260-octet maximum message segment • Uses unique 3-octet routing indicator and provides for multiple addressing for up to 16 destinations • Uses 3 classes of precedence (SysCom, Data1, Data2), in which military precedences (Y-Z-O-P-R) are handled as Data2 • Traffic from subscribers can be limited on precedence; traffic in network is processed by packet precedence • Detects loss of message frames, with notificication for nonperishable messages • Not supported
2	Frame Formatting Frame Addressing Commands & Responses Media Access Data Link Initialization and Release Frame Transfer Acknowledgment (ACK) Retransmission	ISO 3309/7809 (HDLC) with Options 10 and 14 ANSI X3.66-1979 (ADCCP) (MIL188 TRI-TAC Mode VII) ISO 3309 ISO 4335/7809 with addit'l Options 2,4,5,8,11 [5] N/A ISO 4335/7809 ANSI X3.66-1979 (ADCCP) TRI-TAC ICD 16 ISO 4335/7809 ISO 4335 ISO 4335	• Opt 10 calls for extended control field (two octets) • U-frame is extended (two octets) [3] • Opt 14 calls for 32-bit FCS • Station address varies [4] • SIM cmd may be initiated at both stations for link initialization • RIM response not implemented • Does not support poll-final (P/F) bit • When established (initialized), full-duplex point-to-point link has no access contention • Addresses security through use of UI-frames [6] • Uses all 3 types of frames • ACK or NAK is required • Maximum of 5 retries • Retransmission is automatic if no ACK [7]

Table C-2. (Continued)

ISO Layer, Function		Standards Cited	Notes on Interoperability Parameters
1	--Electrical		
	--Voltage Levels	MIL-STD-188-114	[Similar to CCITT V.10/X.26]
	--Load Impedance	MIL-STD-188C	
		MIL-STD-188/24(Prt2)	
		MIL-STD-188-141	
	Mechanical		
	--Connectors	MIL-STD-242G(Prt8)	
		MIL-P-55149	
	Cable Lengths	MIL-STD-242G(Prt8)	
	Functional (pin assign)	MIL-STD-242G(Prt8)	
	Procedural		
	--COMSEC Pre/Postamble		
	Frame Placement	DCT Spec	
	--Keytime Delay	DCT Spec	
	--Bit Synchronization	DCT Spec	
	--Transmission Synch	DCT Spec	
	--Clocking Ctrl & Timing	N/A	

References:

1. Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP), Volume V, Protocol Standard, Headquarters, U.S.Marine Corps, July 1987, UNCLASSIFIED.
2. Discussions with Systems Integration Directorate, MCRDAC, and LOGICON/Eagle Technology, Inc., March 1989.

5. COMPARISON OF TACTICAL PROFILES

5.1 Comparison of US Data Communications Broadcast Protocols Based on HDLC for Digital Entry Devices (DEDs)[7]

Note: STANAG 4202 is used for combat net radio to send STANAG 5500 message text formats. Its interoperability parameters are discussed in Appendix A.

Purpose. This paper compares Marine Tactical Systems[8] (MTS) and Variable Message Format[9] (VMF) broadcast data link layer protocols to High Level Data Link Control[10] (HDLC) and other data link protocols. All of these protocols are candidates for a Digital Entry Device (DED) protocol. This comparison identifies modifications to the base HDLC standard to accommodate a particular feature of a subnetwork technology. It provides insight to the reasons for deviations from the standard.

Background. The VMF data communication data link protocol (Layer 2 of the OSI Reference Model) is being developed for initial use as a broadcast protocol to operate with UHF, VHF, and HF single channel radios.

---

7 This section is based on a contribution from the US Marine Corps, *Comparison of the MTS Broadcast, VMF, and Other Data Link Standards Based on HDLC*, Draft, MCRDAC/Integration (Maj. M. Mascarenas), 15 November 1991, UNCLASSIFIED.

8 *Marine Tactical Systems Technical Interface Design Plan (MTS TIDP)*, Volume V, *Protocol Standard*, US Marine Corps, July 1987, UNCLASSIFIED.

9 *Variable Message Format TIDP*, Volume IV, *Protocol*, February 1991, UNCLASSIFIED.

10 ISO 4335, *High Level Data Link Control (HDLC) Procedures*, Third edition, 1987; ISO 3309, *High Level Data Link Control - Frame Structure*, Third Edition, 1984; and ISO 8885, *High-level Data Link Control Procedures - General-Purpose XID Frame Information Field Content and Format*, First Edition, 1987.

VMF and Air Force Application Program Development[11] (AFAPD) are closely related to the Marine Tactical System (MTS) broadcast protocol. VMF, AFAPD, and MTS are based on ISO 4335 High Level data link control (HDLC) procedures and ISO 3309 HDLC frame structure.

The HDLC standard offers a range of option selections and operating modes that have been used for a variety of station and network types (e.g., point-to-point, multi-link, broadcast). Some of the flexibility built into HDLC includes the following:

- A broad set of commands and responses
- Procedures for primary, secondary and combined stations
- Procedures for half and full duplex
- An extendable control field
- An extendable address field
- A variable information field
- Conventions to allow group and global addressing
- A set of 14 option functions.

Specialized data link standards have been created by selecting from the set of options or through modifications to the HDLC to provide special services. One such modification occurs in the address field. The address field of HDLC only allows one address that identifies the destination of a command and the source of a response. In broadcast type networks that have only combined stations, all stations receive the command or response and any station might have been the originator. Both the source and destination addresses are required to remove any ambiguity. For that reason, data link protocols for broadcast type networks modify the address field to allow at least two addresses, source and destination.

The following are the data link standards that are based on HDLC and used in this comparison:

(1) X.25 LAPB. X.25 LAPB uses the HDLC class of procedures for balanced asynchronous combined (BAC) stations and includes HDLC options 2, 8, and 10. It is intended for point-to-point or multipoint configurations.

(2) ISO 8802-2. ISO 8802-2, Logical Link Control[12] (LLC) defines two modes of operation, connection-oriented (CO) and connectionless (CL), both of which are based on HDLC for BAC stations in a broadcast network. It deviates from the HDLC standard frame format to provide both the source and destination addresses required in a broadcast network. The connection-oriented service uses the basic commands and responses for BAC and adds HDLC options 2, 7 and 10. The connectionless service is a reduced set of commands and responses, but adds HDLC options 1, 4 and 12.

(3) MTS Broadcast. The MTS data link broadcast protocol offers a connectionless service in a broadcast network. It is based on a reduced set of HDLC commands and responses and includes HDLC option 1, 7 and 14. MTS deviates in the address field to include multiple destination addresses for the broadcast network.

(4) ADAPD. AFAPD is based on the MTS broadcast protocol with a change in the address field to provide a mechanism for frame relay.

(5) VMF. VMF is a newly created joint US DoD (under consignment by JTC3A) protocol based on HDLC that is also closely related to both the MTS and ISO 8802-2. It provides both the connection-oriented and connectionless sets of procedures and modifies the definition of both the address and control fields. The connection-oriented set uses the BAC class of procedures and HDLC options 1, 2, 3, 7, 11, and 14. The connectionless operation is identical to the MTS operations.

Discussion. Table C-3 shows a comparison of frame formats and functions performed by the HDLC, X.25 LAPB, ISO 8802-2, MTS, VMF, and AFAPD data link protocols. The following paragraphs discuss each row of Table A-1 to highlight the areas of deviation and to explain the reasons for the deviation.

a. Frame Format. Only ISO 8802-2 varies from the HDLC frame format because it does not have the Frame Check Sequence (FCS) or Flag fields. This is primarily because 8802-2 is used with a Media Access Control (MAC) layer, which provides the FCS and Flag field functions, so the fields in ISO 8802-2 would be redundant.

---

11 *Program Design Specification for the Air Force Application Program Development (AFAPD) for the Digital Communications Terminal (DCT), AN/PSC-2*, US Air Force (TAC/DRI), May 1989, UNCLASSIFIED.

12 ISO 8802-2, *Logical Link Control*, First Edition, 1989.

b. Control Field Size. Only VMF for type 2 service varies from the HDLC standard. A control field exists for each destination address to allow multiple addressing in the connection-oriented mode at the data link (there is no upper layer connection). The sequence windows are different for each of the destination addresses. Therefore, the control field contents are different for each destination. The control field size per destination is a fixed size, one byte.

c. Control Field Size Determination. Only VMF differs from the HDLC standard. In VMF, the size of the control field varies in relation to the number of destination addresses. The control field is composed of 1 to 16 one-byte control subfields. The other standards have control fields that are fixed by agreement to one or two bytes. The VMF variation accommodates multiple addressing in a connection-oriented environment. However, the control field size per destination is determined at initialization, since the VMF standard only allows the SABM (not the SABME) control format that designates the one byte control field.

d. Control Field Formats. All of the HDLC variants choose the formats from the complete set of HDLC formats according to the needs of the protocol. All of the connection oriented protocols (LAPB, and Type 2 services in ISO 8802-2 and VMF) use the basic set of control field formats and one or more from the optional formats. The connectionless mode protocols (MTS and Type 1 services in ISO 8802-2 and VMF) use a subset of the HDLC basic control field formats, because those pertaining to the connection set-up, maintenance, and disconnect are not required.

e. Address Field Size. A variance in this field is allowed by the basic HDLC protocol. While the size of the address can vary according to the HDLC standard, only one address is allowed. ISO 8802-2, MTS, AFAPD, and VMF have all extended the address field for the purpose of including the source address as well as the destination address. Those protocols are not point-to-point so the source is not obvious (as it is in the LAPB point-to-point protocol). MTS, VMF, and AFAPD have further extended the field to allow multiple destination addresses (an expansion of the group address). MTS, AFAPD, and VMF use the HDLC method [least significant bit (LSB) indicator] to extend the field. ISO 8802-2 uses the LSB for another purpose but has a fixed size address field. AFAPD further extends and modifies the address field to provide a frame relay function. The length of the field depends of the number of destinations and the use of the relay function.

- MTS, AFAPD, and VMF use the HDLC address extension method (LSXB) to lengthen the address field. Within the longer field, MTS and VMF identify subfields for the source and one or more destination addresses. ISO 8802-2 defines two address fields that are each one byte long. ISO 8802-2 does not use the LSB to indicate the extended address field. That bit indicates a group address in the destination address, and a command or response in the source address.
- VMF designates an address (value = 1) to have additional special significance within that protocol. The address equal to 1 is used to indicate the frame is in the Type 2 service format. (ISO 8802-2 also allows both Type 1 and Type 2 service. The service types are distinguishable in ISO 8802-2 because they contain exclusive sets of control field formats.)

Table C-3. Comparison of Example Broadcast Protocols with HDLC, X.25 LAP B, and LLC

	HDLC 7809 BAC	X.25 LAP B	802.2 LLC	MTS BROADCAST	VMF	AFAPD
Frame Format	Flag Address Control Info CRC Flag	Same	DSAP, SSAP Control, Info	Same	Same	Same
Control Field Size	Extendable 1 or 2 Bytes for I PDU and S PDU. 1 Byte for S PDU	Same	2 Bytes for I PDU and S PDU. 1 Byte for U PDU.	1 Byte only	1 Byte only	1 Byte only
Control Field Size Determination	At Link Set-Up	At Link Set-Up	Fixed	Fixed	Fixed	Fixed
Control Field Formats	(If no options) Comm Resp I I RR RR RNR RNR SABM UA DISC DM FRMR with options add: SABME XID XID SREJ SREJ UI UI REJ REJ SIM RIM UP TEST TEST RSET RD	Comm Resp I I RR RR RNR RNR SABM UA SABME DM DISC FRMR	Type 1 Comm Resp UI XID XID TEST TEST Type 2 I I RR RR RNR RNR SABME UA DISC DM REJ FRMR RSET REJ	Comm Resp I RR RR RNR RNR XID XID	Type 1 Comm Resp I RR RR RNR RNR XID XID Type 2 I I RR RR RNR RNR SABM UA DISC DM REJ FRMR SREJ	Same as MTS
Address Field Size	Extendable 1 to XX Bytes	1 Byte	2 Bytes	2-17 Bytes	2-17 Bytes	3-20 Bytes
Address Field Formats	Source: None Destination: Global = 11111111 Group = by Agreement No Station = 0 Range = 0-255 or 0-127 if Extended	11000000 or 10000000	Source: 7 Bits 1-126 Destination: Global = 11111111 Group = 1XXXXXXX No Station = 0 Range = 0-127	Source: 7 Bits 1-126 Destination: Global = 11111111 No Station = 0 Range = 0-127	Source: 7 Bits 2-95 Destination: Global = 11111111 Group = XXXXXXX1 No Station = 0 Special = 1 Range = 0-127	Source Originator Direct Destination Relay Flag Hop Count Relay Destin- ation
Address Field Size Determination	LSB	Fixed	Fixed	LSB	LSB	LSB and Relay Function

Table C-3. (Continued)

	HDLC 7809 BAC	X.25 LAP B	802.2 LLC	MTS BROADCAST	VMF	AFAPD
Info Field Size Max	Any # of Bits	259 Bytes	Any # of Bytes	3500 Bytes	Negotiable Max = 3500	3500 Bytes
FCS	16 Bit or 32 Bits (Option #14)	16 Bit	None	32 Bit	32 Bit	32 bit
P/F Bit	P - One outstanding Request F - Set in response to received P Bit	Same	Same	Same except for the XID exchange	Same	Same
Sequence Numbers	0-7 or 0-127	0-7 or 0-127	0-127	Not Used	0-7	Not Used
Link Set-up Disc	SABM → UA SABME → UA DISC → UA	SABM → UA or SABME → UA DISC → UA	Type 1 Not Used Type 2 SABME → UA DISC → UA	Not Used	Type 1 SABM → UA DISC → UA Type 2 Not Used	Not Used
Network Control	XID	None	Type 1 XID Type 2 None	XID	Type 1 XID Type 2 XID	Not Used

- AFAPD address field content is identical to MTS if there is no relay destination. However, the address field has several additional subfields for the relay function. there are two source addresses instead of one (the originator and the current transmitting link address) and two destination fields (the final destination and a relay destination). There are three additional subfields (relay, flag, and hopcount) that are used in the relay process.

g. Address field size determination. ISO 8802-2 deviates from HDLC because it defines two separate address fields of one byte each. It does not use the LSB to indicate an address field longer than one byte. AFAPD field size depends on the number of destination and if relay is requested.

h. Information Field Size Maximum. Each protocol adheres to the HDLC standard because HDLC allows any information field size.

i. FCS. ISO 8802-2 does not use the FCS field because the LLC is used with a MAC layer which provides the FCS functions. All of the other protocols use either the basic (16 bit) or optional (32 bit) FCS as allowed by the HDLC standard.

j. P/F Bit. MTS broadcast protocol follows the P/F standard for I-frame exchanges, but not in the XID exchange.

k. Sequence numbers. ISO 8802-2 MTS, and VMF do not use sequence numbers in the connectionless-mode of service. Sequence numbers are used for flow control and sequencing that are not functions of the CL service.

l. Link Set-up and Disconnect. All of the protocols that provide a connection-oriented service adhere to the HDLC standard for the link set-up and disconnect. The connectionless service mode in MTS, VMF, and ISO 8802-2 do not perform this function.

m. Link Control. The XID command is an optional command and response in HDLC. ISO 8802-2 and VMF use the XID format to pass link control information in the information field according to ISO 8885 - HDLC procedures - General purpose XID frame information field content and format. MTS and AFAPD use the XID with a one-byte information field for link initialization but do not follow ISO 8885 rules to identify the XID information field content.

5.2 Comparison of US Data Communications Broadcast Protocols Planned for Use in Land Warfare Fire Support CCISs[13]

Overview. MTS broadcast standard, VMF, and AFS-BOM[14] are all bit-oriented communication protocols that have a data link layer to support combat net radio, a broadcast communicators medium. VMF and AFS-BOM were produced in parallel with the same Army and Marine Corps representatives and are based on the MTS protocol. In fact, the VMF specification was written using the MTS TIDP, Volume V, as the beginning text. This section compares the functional differences among the MTS, VMF, and AFS-BOM protocols and evaluates their ability to interoperate.

Functional Differences. Table C-4 lists the functions performed at each of the layers and briefly states the differences among the protocols.

a. Physical Layer. There are no functional differences among the protocols in this layer.

b. Data Link Layer. Listed below are three functional differences among the protocols.

- Media Access. The VMF protocol implements both a random and a prioritized method of calculating the net access delay (NAD) time. MTS only implements the random method, and AFS-BOM only implements the prioritized method. Since VMF implements both schemes, the different media access schemes only create an interoperability problem between the MTS and AFS-BOM protocols. Since the VMF protocol was developed to provide Marine Corps and Army fire support interoperability, there is not a problem.
- Connection Establishment and Release. An XID exchange is currently being developed for the VMF protocol that will be incompatible with either the MTS or AFS-BOM XID exchange. It is unknown at this time whether AFS-BOM will incorporate this change. In any case, the XID is not mandatory for initialization, so this difference will not prohibit interoperability.
- Acknowledgement. During development of the VMF and AFS-BOM protocols, a change was made to the list of conditions that must be met in a frame before the data link layer will transmit acknowledgement of the frame. This change only affects the action *within* an end system and is not related to interoperability.

c. Network Layer. While the MTS broadcast protocol allocates space or the network header, it is not functional. For this layer only, the functionality of the MTS switched protocol will be compared to the other protocols. See Table A-2. The differences are listed below.

- Message Types. In the VMF and AFS-BOM protocols the message type field defines a more expansive list of message types. The same division of SYSCON, perishable, a non-perish-able messages remains, however, so there is no related interoperability problem.
- Routing. VMF and AFS-BOM both allow a destination source list to be present in the network header. MTS switched protocol would interpret this list as multiple destinations rather than a routing list. MTS, VMF, and AFS-BOM are not interoperable when more than one destination address is present in the header.
- Message Segmenting. MTS (broadcast) and VMF do not allow a message to be segmented. AFS-BOM segments messages over 3,500 bytes. This is not currently a problem because the broadcast medium allows a frame size of 3,500 bytes, which is more than the longest message. Segmentation is not necessary.
- Originator and Addressee. The MTS uses the principle of a 3-byte geographically hierarchical address or fixed addresses. The description of its use is difference because the routing function has been moved from the switches into end systems in the broadcast medium.

d. Transport Layer. There are not functional differences among the protocols in this layer.

---

13 This section is based on a contribution from the US Marine Corps, *Comparison of the Marine Tactical System (MTS(, Variable Message Format (VMF), and Army Fire Support Bit-Oriented Message (AFS-BOM) Protocols,* Draft, MCRDAC/Integration, 15 November 1991, UNCLASSIFIED.

14 Army Fire Support Bit-Oriented Message (AFS-BOM) Protocol, US Army Field Artillery School, 1990.

Table C-4. Comparison of Protocol Functions

FUNCTIONS	MTS	VMF	AFS
Physical Layer			
Electrical			
Mechanical			
Functional			
Procedural			
Link Layer			
Frame Formatting			
Frame Addressing			
Commands and Responses			
Media Access	Random	Random & Prioritized	Prioritized
Connection Establishment & Release	One XID exchange	2 new XID exchanges	?
Frame Transfer			
Acknowledgement	Verifies data pattern	Does not verify data pattern	Does not verify data pattern
Retransmission			
Error Detection & Correction			
Network Layer			
Header	* 3 message types	9 message types	9 message types
Routing	* Directory	Directory & Source	Directory & Source
Message Segmenting	* Yes	none	Yes
Packet Addressing	*		
Packet Precedence	*		
Network Flow and Cogestion Control	*		
End-to-End Error Recovery	*		
Transport Layer			
Null			
Session Layer			
Presentation Layer			
Message Formatting	Format 3	Format 3	Format 1, 2, and 3
Application Layer			
Message Header			Different bit interpretation of message number field
Message Acknowledgement			
System Management	*		

* Function is present in the MTS switched protocol, but not in the MTS broadcast protocol.
Blank fields indicate that all of the protocols implement the function the same.

e. Presentation Layer. MTS and VMF only allow Type 3 VMF message format, but AFS-BOM will a also allow VMF message formats of Types 1 and 2. AFS-BOM will not send Type 1 or Type 2 message either MTS or VMF protocols, so this layer will be interoperable.

f. Application Layer. The message number field in the header contains a different data element structure in each of the protocols. In both MTS and VMF, message number is 17-bit field made up of a 7-bit functional area element and a 10-bit number element. MTS interprets the functional area as an ASCII character and VMF as a numeric. AFS-BOM divides the 17-bit message number field into a 3-bit format designator element, a 4-bit functional area element and a 10-bit number element. AFS-BOM will zero fill the 3-bit format designator element to achieve interoperability with VMF. MTS would not recognize VMF or AFS-BOM message numbers.

6. FRENCH CCIS INITIATIVES[15]

6.1 RITA (Réseau Intégré de Transmission Automatique)

RITA is a tactical integrated communication network for the deployed Army, which offers the following services between static or mobile users:

- Telephony
- Telegraph (with encoding facilities)
- Facsimile
- Data transmission.

This system is being improved in order to take into account new operational needs. In particular, new standardized numeric services are under development as well as the interconnection with other networks (PR4G, SOCRATE, SYRACUSE).

The following standards are implemented at the interface level:

- NATO interconnection: STANAG 4206, 4211, 4249, and X.75M
- ISDN networks: T2 interface and D protocol.

6.2 RITTER (Réseau Intégré de Transmission de l'Armée de Terre)

The aim of RITTER is to meet the French Army strategic telecommunication needs and to enable interoperability with other national networks and with NATO networks. The following functionalities are offered:

- Telephonic switching
- Data transmission (X.25)
- Hierarchically organized network management.

The numeric support implements the CCIR standards, and X25 transmissions carry the telegraphy and X400 Military MHS.

6.3 SOCRATE

The aim of the SOCRATE project is to build an inter-army backbone telecommunications network, implementing the most recent numeric technologies. This program consists of a fusion of RA90 and RITTER programs in a single and coordinated realization. SOCRATE will offer services that include the following:

- Telephony
- Data transmission
- MHS
- Telex
- Still and moving picture transmission.

SOCRATE will also guarantee the communications security. It will provide a national covered network built upon an ATM multiservice switching system that is based upon electro-magnetic waves and fibre-optic sections. Access to SOCRATE will be accomplished via ATM, ISDN, and X.25 protocols, as well as via G703 interface.

6.4 SYRACUSE

SYRACUSE is a transit network composed of an earth component and a spatial component (satellite). It enables communications between armies inside the area covered by the satellite, using telephony, telegraphy, and data transmission services.

6.5 NTIA (Inter-Army Transit Node)

With the aim of improving the internetworking, the creation of an inter-army transit node has been decided. The NTIA is a unique gateway between actual or future networks (see Figure C-8). The exchange protocols are based upon the X.75 protocol.

[15] Based on [FR MOD 1994], February 1994.

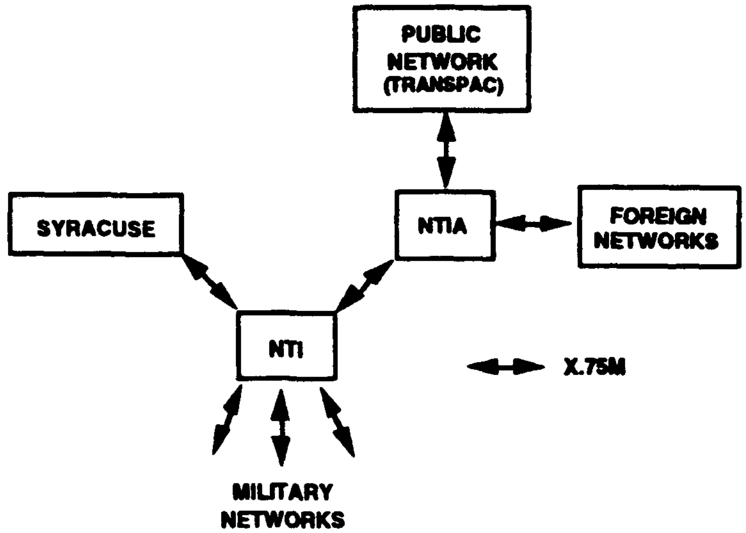


Figure C-8. French Internetworking Concept

6.6. RAMSES and TELEMAC

RAMSES and TELEMAC are both application-oriented networks which use the inter-army telecommunication networks SYRACUSE and RETIAIRE (X.25). These systems offer secure services for telephony, data transmission, MHS (X400) and picture transfer.

6.7 ENTAME

ENTAME is a French secured inter-army message handling system based on the ACP 127 procedure. The message format is ADat-P3 conformant. ENTAME uses various military networks (RTDM, RETINAT, RESEDA) and the TELEX network.

APPENDIX D

INTERNATIONAL CIVIL STANDARDS RELEVANT TO INFORMATION SYSTEMS

INTERNATIONAL CIVIL STANDARDS RELEVANT TO INFORMATION SYSTEMS BY LAYER OF OSI REFERENCE MODEL[1]

I. OSI ARCHITECTURE AND GENERAL STANDARDS[2]

A. OSI Basic Reference Model and Conventions
B. Work Plans and Coordination Agreements
C. Formal Description Techniques (FDTs)
D. Security
E. OSI Management
F. OSI Registration Authorities
G. OSI Conformance Testing
H. Taxonomy and Profiles
I. Modelling Facilities
J. Open System Environment (OSE) and Programming Interfaces

A. OSI BASIC REFERENCE MODEL AND CONVENTIONS:

STANAG[3] 4250◆	NATO Reference Model for OSI	
	Part 1--General Description, Draft, Edition 2	
	Part 2--Security, Draft	
	Part 3--Naming and Addressing, Draft	
	Part 4--Management, Draft	
ISO 7498◆	OSI Reference Model, Part 1: Basic Reference Model, General Aspects (X.200:1988)	
	Cor[4] 1	Technical Corrigendum 1
	AD[5] 1◆	Connectionless-Mode Transmission
	PDAD[6] 2◆	Multipeer Data Transmission (MPDT) (suspended)
ISO/IEC 7498-1:1994	OSI Reference Model, Part 1: General Aspects, Edition 2 (X.200)	
ISO 7498-2◆	OSI Reference Model, Part 2: Security Architecture (X.800)	
ISO 7498-3◆	OSI Reference Model, Part 3: Naming and Addressing (X.650)	
ISO/IEC 7498-4◆	OSI Reference Model, Part 4: Management Framework (X.700)	
WD[7] 7498-5	OSI Reference Model, Part 5: Architecture for Multi-Peer Communications	
ISO/TR[8] 8509◆	Service Conventions (X.210:1988)	
ISO/TR 9575◆	OSI Routing Framework	
ISO/IEC TR 10730◆	Tutorial on Naming and Addressing	
	WDAM 1	Amendment 1: Directory Names
ISO/IEC 10731◆	Conventions for Definitions of OSI Services (X.210:1993)	
ISO/IEC TR 12178	User Requirements for Systems Supporting Time-Critical Communications	
ITU-TS X.200	Reference Model: Basic Reference Model (ISO/IEC 7498), 1988	
ITU-TS X.210:1988	OSI Layer Service Definition Conventions (ISO 8509), 1988	
ITU-TS X.210:1993	Conventions for Definitions of OSI Services (ISO/IEC 10731), Draft, 1993	
ITU-TS X.220 Rev 1	Use of X.200 Series Protocols in CCITT Modifications, 1993	

---

1 Based on the following:
a. *ISO/IEC JTC1/SC 21 Programme of Work* [SC21 N 8082 1993]
b. September 1993 *NOSIP Strategy* [NATO 1993]
c. Private communication from UK's Defence Research Agency [DRA 1993]
d. Aditional contributions from the nations participating in the ATCCIS PWG.

2 The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

3 STANAG: NATO Standardization Agreement

4 Cor.: Technical Corrigendum to ISO standard.

5 AD: Addendum for ISO standard.

6 PDAD: Proposed or Preliminary Draft Addendum to ISO standard.

7 WD: Working Draft for ISO (status of text prior to being submitted as a Committee Draft).

8 TR: Technical Report for ISO.

ITU-TS X.650	OSI, Basic Reference Model: Naming and Addressing (ISO 7498-3), 1992
ITU-TS X.700	Management Framework for Open Systems Interconnection (OSI) for CCITT Applications (ISO 7498-4), 1992
ITU-TS X.800	Security Architecture for Open Systems Interconnection for CCITT Applications (ISO 7498-2), 1991
Working Papers on Reference Models and Architecture	
SC21 SD-9[9]	Approved Commentaries on the Basic Reference Model for Open Systems Interconnection, SC21 OSI Reference Model Editor
SC21 N 5934	Collection of Definitions of OSI Vocabulary (April 1991 Version), Rapporteur on Q17: OSI Vocabulary
SC21 N 6069	Proposed New WG6 Question Q6/2 on the Relationship Between the OSI Upper Layer Architecture and ODP
SC21 N 6070	Working Draft Answer to the Proposed WG6 Question on the Architectural Relationship Between OSI and ODP
SC21 N 6157	Answer to CCITT SG VII Q 23 on OSI Reference Model Regarding ISDN
SC21 N 6198	Approved Commentaries on the OSI Basic Reference Model
SC21 N 6808	Organization of Work on OSI and ODP Architecture UK National Body
SC21 N 6902	Liaison Statement to SC21 on Revision of the OSI Reference Model
SC21 N 7093	Proposed New Question Q1/68 on the Definition of the Term "Application-Process-Title" in the OSI Reference Model
SC21 N 7094	Draft Answer to Q1/68 - Definition of the Term "Application-Process-Title" in the OSI Reference Model
SC21 N 8265	Liaison Statement to SC21 on OSI Service Conventions, ITU-TS SG7, October 1993
SC21 N 8266	Liaison Statement to SC21 on OSI Reference Model, ITU-TS SG7, October 1993
Working Papers on Multicasting (Multipeer Data Transmission)	
SC21 N 3711	Requirements for Multipeer Data Transmission
SC21 N 3906	Final Report to SC21 in Florence on the Reassessment of Project JTC 1.21.9.1 on Multipeer Data Transmission
SC21 N 4681	User Requirements for Multi-Party Communications (MPC), Canada
SC21 N 6197	WG1 Position on the Reactivation of Project 1.21.9.1 (Multi-Peer Data Transmission)
SC21 N 6793	Proposed Mechanism for Soliciting National Body Input on Multipeer/Multicast Application Requirements
SC21 N 6794	Preliminary Requirements for a Multipeer Data Communication Architecture
SC21 N 6812	Request to Apply the Procedures for the Reactivation of the Multi-Peer Data Transmission Project (MPDT)
SC21 N 6813	Draft Addendum for Multi-Peer Data Transmission Project (MPDT)
SC21 N 6814	Liaison Statement to SC21 on Lower Layer Multicast Work SC6 Enhanced Transport Mechanisms Meeting
SC21 N 6948	Responses to the Proposed Mechanism for Soliciting National Body Input on Multipeer/Multicast Application Requirements
SC21 N 6961	SC21/WG1 Decision on MPDT Reactivation
SC21 N 7062	Liaison Statement to SC6 on Multipeer Data Transmission
SC21 N 7063	Liaison Statement to CCITT SG VII on Multipeer Data Transmission
SC21 N 8003	NP on Architecture for Multipeer Data Communications
SC21 N 8267	Liaison Statement to SC21 on OSI Multicast Architecture, ITU-TS SG7, October 1993
SC21 N 8384	Liaison Statement to SC21/WG1 on Multi-Peer Data Transmission, ISO/TC184/SC5/WG2, December 1993
Working Papers on Quality of Service	
SC21 N 5110	Call to National Bodies and Liaison Organizations for Contributions on Technical Structure of Quality of Service (QOS) Architecture
SC21 N 6158	Final Answer to Q1/62 (Quality of Service Architectural Issues)
SC21 N 6159	Framework on Quality of Service
SC21 N 7066	Liaison Statement to SC6 Concerning Quality of Service (QOS)
SC21 N 7067	Results of the SC21/WG1 Meeting on Quality of Service
SC21 N 7991	Liaison Statement to JTC1/SC18, SC25, SC27, SC29, ISO/TC68, ISO/TC46, and JTC1/WG3 Concerning Activity on Quality of Service, SC21/WG1, August 1993
SC21 N 7992	Liaison Statement to ISO/TC184/SC5/WG2 Concerning Activity on Quality of Service, SC21/WG1, August 1993
SC21 N 7993	Quality of Service Framework, second working draft
SC21 N 8005	Liaison Statement to ITU-TS/SG7 (Q2/7, Q19/7, Q20/7) on Quality of Service, SC21/WG1, August 1993

9 SD: Standing Document for an ISO subcommittee.

SC21 N 8029	Liaison Statement to JTC1/SC6 on Quality of Service, SC21/WG1, August 1993
SC21 N 8030	Liaison Statement to EWOS, OIW, and AOW on Quality of Service, SC21/WG1, August 1993
SC21 N 8262	Liaison Statement to SC21 and SC6 on OSI Quality of Service, ITU-TS SG7, October 1993
SC21 N 8263	Liaison Statement to SC21 and SC6 on OSI Quality of Service Framework Specifications, ITU-TS SG7, October 1993
Working Papers on Protocol Efficiency	
SC21 N 6906	Liaison Statement to SC21 on Efficiency of OSI Protocols
SC21 N 8018	Liaison Statement to ITU-TS SG7 (Q19/7) on Q1/65.2—OSI Protocols Efficiency, August 1993
SC21 N 8268	Liaison Statement to SC21 WGs 1 and 8 on OSI Protocol Efficiency to ICG on Satellite Matters, SG8, SG11, SG13, ISO/IEC JTC1/SC21 (WGs 1 and 8), and ISO/JTC1/SG6, ITU-TS SG7, October 1993
Working Papers on Time Critical Communications	
SC21 N 8004	Liaison Statement to ISO/TC184/SC5/WG2 on Question 65.1—User Requirements for OSI Systems Supporting Time Critical Communications, SC21/WG1, August 1993
SC21 N 7090	Proposed New Question Q1/65 on User Requirements for OSI Systems Supporting Time Critical Communications
SC21 N 8382	Liaison Statement to SC21/WG4 on Management of Time Critical Communications, ISO/TC184/SC5/WG2, December 1993
SC21 N 8383	Liaison Statement to SC21/WG1 on Question 65.1—User Requirements for OSI Systems Supporting Time Critical Communications, ISO/TC184/SC5/WG2, December 1993
SC21 N 8385	Final Draft Version of TCCA Technical Report (DTR 12178) Sent to the ISO Central Secretariat for Publication, ISO/TC184/SC5/WG2, December 1993
Working Papers—Time Service	
SC21 N 6749	Proposal for a New Work Item on Information Technology - Text Communication - Coordinated Time Service in an OSI Environment
SC21/WG4 N 1451	Comments on SC21 N 6749: NP Time Services in an OSIE

B. WORK PLANS AND COORDINATION AGREEMENTS:

Standing Documents	
SGFS SD-4	Framework and Taxonomy of International Standardized Profiles - Directory of ISPs and Profiles Contained Therein, SGFS N 1049, November 1993
SGFS SD-7	Issues List for Future Development of ISO/IEC TR 10000, SGFS N 1023, September 1993
SC21 SD-1	Report of the SC21 Secretariat, SC21 Secretariat, January 1993
SC21 SD-2	ISO/IEC JTC1 SC21 Programme of Work (POW) - Target Date Summary for All Active and Published Projects, SC21 Secretariat, October 1993
SC21 SD-3	SC21 Inter-Project Dependencies, SC21 Secretariat, May 1992
SC21 SD-4	SC21 Strategic Plan, January 1992
SC21 SD-5	Rules to be Applied in the SC21 Editing Process, November 1991
SC21 SD-6	Directives for the Work of JTC1, Edition 2, 1992
SC21 SD-7	Management Plan for Security, Edition 1, June 1990
SC21 SD-8	SC21 Schedule of Meetings, June 1993 [SC21 N 8084]
SC21 SD-9	Approved Commentaries on the Basic Reference Model for Open System Interconnection, OSI Reference Model Editor, November 1991
SC21 SD-10	SC21/ITU-TS Collaborative Projects, September 1993
SC21 SD-11	Management Guidelines for SC21, December 1993 [SC21 N 8362]
Guidance	
SC21 N 7215	Management Guidelines for SC21, June 1992 (to be updated in accordance with SC21 N 8122)
SC21 N 7489	Guide for ITU-TS (CCITT) and ISO/IEC JTC1 Cooperation, December 1992 (Annex K to the ISO/IEC JTC1 Directives, JTC1 N 2119)
SC21 N 8116	Final Steps for the Editing of Standards in the Case of Collaborative Work with ITU-TS, June 1993
SC21 N 8080	Guidelines for Conducting Editing Meetings Using Electronic Mail, June 1993
SC21 N 8132	Identification of Versions in the Foreword of a Standard, June 1993
SC21 N 8024	Programme of Work of ISO/IEC JTC1/SC21/WG1, June 1993
SC21 N 8249	Rules of Procedure and Working Methods of the ITU Telecommunications Standardization Sector and Study Group Responsibility and Mandates, ITU-TS, October 1993
SC21 N 8410	Methodology and Guidelines for the Development of Application Layer Protocols
Reports for 1994 JTC1 Plenary Meetings	
JTC1 N 2642 Rev.	Calling Notice and Draft Agenda for the First Meeting of ISO/IEC JTC1/SC21 Joint Working Group 9, Corrected Version, SC21 Secretariat, September 1993 (to process the interpretation of ISO/IEC Guide 25 for Information Technology Testing Laboratories for Software and Communications Testing Services [JTC1 N 2527] and produce a revision for balloting as a draft technical report; held 30 November to 2 December 1993 in London)
JTC1 N 2775	Summary of Voting on Document JTC1 N 2621, Proposal for a New Work Item: Conceptual Schema Modelling Facility, December 1993

JTC1 N 2835	Report from ISO/IEC JTC1/SC21 Chairman on Activities Related to Application Program Interfaces (APIs) and Modelling Facilities (MFs), January 1994
JTC1 N 2836	JTC1/SC21 Reports on Application Program Interfaces (APIs), January 1994
JTC1 New Work Item Proposals	
JTC1 N 960	Proposal for an NWI: Management Information Register and Registration Procedure (in June 1993, SC21 recommended to JTC1 that the project be cancelled [SC21 N 7944])
JTC1 N 2246	Proposal for an NWI: Command Sequencer (comments on JTC1 ballot were resolved by SC21 in June 1993 and the revised NWI proposal forwarded to JTC1 for consideration [SC21 N 7943])
JTC1 N 2248	Proposal for an NWI: Enhancement of Directory Operational Security (comments on JTC1 ballot were resolved by SC21 in June 1993 and the revised NWI proposal forwarded to JTC1 for consideration [SC21 N 7933]) (revisions to nine parts of ISO 9594 and possibly one new part; WDs expected February 1994, CDs November 1994, DISs May 1995, and ISs May 1996)
JTC1 N 2249	Proposal for an NWI: Removal of Session Layer Serial Number Limitation (comments on JTC1 ballot were resolved by SC21 in June 1993 and the revised NWI proposal forwarded to JTC1 for consideration [SC21 N 7985])
JTC1 N 2264	Proposal for an NWI: Extensions to ACSE Covering ASOs and ASO-Associations (comments on JTC1 ballot [JTC1 N 2507] were resolved by SC21 by revising the scope of work; the project has been added to SC21 program of work [SC21 N 8076])
JTC1 N 2612	Proposal for an NWI: Open Systems Assessment Methodology, August 1993 (failed to qualify for JTC1 program of work, as five P-members do not commit to active participation [JTC1 N 2773, December 1993])
JTC1 N 2620	Proposal for an NWI: Conformance Testing of OSI Protocols Over OSI Services Provided by Non-OSI Protocols, August 1993 [SC21 N 8011, June 1993] (failed to qualify for JTC1 program of work, as five P-members do not commit to active participation [JTC1 N 2774, December 1993])
JTC1 N 2621	Proposal for an NWI: Conceptual Schema Modelling Facility, August 1993 [SC21 N 8060, June 1993] (balloting ended in November 1993) (WD expected July 1995, CD July 1996, DIS July 1997, and IS July 1998)
JTC1 N 2760	Proposal for an NWI: Amendment to ISO/IEC 8473-1 Covering Extensibility and Quality of Service, December 1993 [SC6 N 8518, November 1993] (balloting ends 16 March 1994) (PDAM to ISO/IEC 8473-1 expected October 1993, DAM March 1994, and AM November 1994)
JTC1 N 2769	Proposal for an NWI: Extension to ISO/IEC 8072 for Protection Quality of Service, December 1993 [SC6 N 8560, November 1993] (balloting ends 1 April 1994)
JTC1 N 2801	Proposal for an NWI: ISO/IEC 7498-n, Architecture for Multipeer Communications [SC21 N 8003] (balloting ends 29 March 1994) (new part to ISO 7498; WD expected in 1995, CD in 1996, DIS in 1997, and IS in 1998)
JTC1 N 2802	Proposal for an NWI: Enhancements to LOTOS, December 1992 [SC21 N 8022] (balloting ends 29 March 1994) (PDAM to ISO 8807 expected June 1995, DAM June 1996, and AM June 1997)
JTC1 N 2803	Proposal for an NWI: Directory Schema Migration, December 1992 [SC21 N 7942] (balloting ends 29 March 1994) (revisions to nine parts of ISO 9594; WDs expected July 1994, CDs November 1994, DISs May 1995, and ISs May 1996)
Reports, Resolutions, and Recommendations from SC21 Plenary Meetings	
JTC1 N 2707	Proposed Modifications to the ISO/IEC JTC1/SC21 Programme of Work, Secretariat, ISO/IEC JTC1/SC21, November 1993
JTC1 N 2777	Report of JTC1/SC21 to the 1994 JTC1 Plenary Meeting in Washington, DC, Secretariat, ISO/IEC JTC1/SC21, December 1993
JTC1 N 2851	Management Report of JTC1/SC21 to the 1994 JTC1 Plenary Meeting in Washington, DC, Chairman, ISO/IEC JTC1/SC21, January 1994
SC21 N 7978	Rationale for Proposed SC21/WG4 Program Extensions, SC21/WG4, July 1993
SC21 N 7979	Report of the Tenth ISO/IEC JTC1/SC21/WG4 Meeting, Yokohama, 15-24 June 1993, SC21/WG4, September 1993
SC21 N 8021	Report of the ISO/IEC JTC1/SC21/WG1 Meeting, Yokohama, 16-24 June 1993, SC21/WG1, September 1993
SC21 N 8024	ISO/IEC JTC1/SC21/WG1 Programme of Work, SC21/WG1, July 1993
SC21 N 8027	Resolutions of SC21/WG1, June 1993
SC21 N 8028	List of Late Contributions and Output Documents of the SC21/WG1 Yokohama Meeting, 16-24 June 1993, SC21/WG1, July 1993
SC21 N 8081	Resolutions of the Ninth Plenary Meeting of ISO/IEC JTC1/SC 21, 29-30 June 1993, Yokohama, Japan, June 1993
SC21 N 8123	Resolutions of SC21/WG3, June 1993
SC21 N 8217	Report of the SC21/WG7 Meeting, June 1993, Yokohama, SC21/WG7, September 1993
SC21 N 7977	Resolutions of SC21/WG4, June 1993
SC21 N 8055	Resolutions of SC21/WG7, June 1993
SC21 N 8078	Resolutions of SC21/WG8, June 1993
SC21 N 8085	Convenor's Report for SC21/WG1, June 1993
SC21 N 8115	Convenor's Report for SC21/WG3, June 1993

SC21 N 8043	Convenor's Report for SC21/WG4, June 1993
SC21 N 8124	Convenor's Report for SC21/WG7, June 1993
SC21 N 8079	Convenor's Report for SC21/WG8, June 1993
EWOS Technical Guides	
EWOS SD17	Generic Terms of Reference for EWOS Expert Groups, November 1993
EWOS ETG 001	FTAM - Tutorial on Rules for ASN.1 Encoding, April 1989
EWOS ETG 003	FTAM - Remote Actions (RA) over FTAM, Service and protocol, Edition 2, May 1992
EWOS ETG 005	Introduction to Directory Profiles, Edition 3, May 1993
EWOS ETG 007	FTAM - Service Classes and Functional Units in ENV 41 205, Edition 2, August 1990
EWOS ETG 008	Procedures and Evaluation Criteria for Standardization of Test Specifications for European Functional Standards, October 1990
EWOS ETG 009	Conformance Vocabulary, Edition 2, September 1992
EWOS ETG 010	Conformance Tutorial, January 1991
EWOS ETG 011	Tutorial for Directory Q-Profile Production, January 1991
EWOS ETG 013	A Mapping of the X-Window System over an OSI Stack, May 1991
EWOS ETG 016	PTS Specification, February 1992
EWOS ETG 017	Error Handling in Directory, May 1992
EWOS ETG 018	OSI TP Tutorial, Part 1, September 1992 and Part 2, May 1993 (separate volumes)
EWOS ETG 020	PTS Maintenance Procedures, September 1992
EWOS ETG 022	Organization of Common PTS, November 1992
EWOS ETG 025	The TTCN Style Guide and Quality Criteria, November 1993
EWOS ETG 026	Role of Standards in OSI Testing, Edition 2, February 1993
EWOS ETG 027	Security Architecture for the Directory, February 1993
EWOS ETG 028	Interoperability - Vocabulary, May 1993
EWOS ETG 029	Interoperability - Classification, May 1993
EWOS ETG xxx	Library of Test Specifications, Draft (ETG expected November 1993)
EWOS ETG xxx	Technical Guide to ISO 9646 Test Environment, Draft (ETG expected November 1993)
EWOS ETG xxx	Interconnection of Directory Domains (DMD-DMD), Draft (ETG expected November 1993)
EWOS ETG xxx	Methodology Handbook for PTS Production, Draft (replaces ETG 008; ETG expected February 1994)
EWOS ETG xxx	Test Report Proformas, Draft (ETG expected February 1994)
EWOS ETG xxx	Development of Taxonomy for DBE Requirements, Draft (ETG expected March 1994)
EWOS ETG xxx	Technical Framework for Security-Related Profile Development, Draft (ETG expected May 1994)
EWOS ETG xxx	Application of Security Techniques to Base Standards, Draft (ETG expected May 1994)
EWOS ETG xxx	User Requirements for More DBE Profiles, Draft (ETG expected September 1994)
EWOS ETG xxx	Policy Statement on the Role of Standards in OSI Testing, Draft
Regional Workshop Technical Reports	
RWS-TR 001	Guiding Principals for Regional Requirements
RWS-TR xxx	Guidelines for Managed Object Profiling and Taxonomy (EWOS), November 1993 (RWS-TR expected February 1994)
RWS-TR xxx	Framework for Conformance Testing of Network Management Profiles (EWOS), September 1993 (RWS-TR expected February 1994)
RWS-TR xxx	Registration of Object Identifiers in ISPs (EWOS SD-16; EWOS approval expected March 1994)
RWS-TR xxx	Conformance Testing Vocabulary (EWOS approval expected May 1994)
RWS-TR xxx	TTCN Style Guide (EWOS approval expected November 1994)
RWS-TR xxx	Library of Test Specifications (EWOS approval expected November 1994)
RWS-TR xxx	Guidelines for Managed Object Harmonization (EWOS approval expected November 1994)
RWS-TR xxx	Ensembles Guidelines (EWOS approval expected November 1994)
RWS-TR xxx	Test Case Selection Rules (OIW)
Other Documents—SGFS	
SGFS N 1003	Modification of SD-1, SGFS Procedures, for Adoption of PTSs and APIs, August 1993
SGFS N 1043	Liaison Statement to SGFS and EWOS/EG-OSE, OIW, November 1993
SGFS N 1065	US Comments on OIW Liaison Statement to SGFS and EWOS/EG-OSE, August 1993
SGFS N 1087	Liaison Statement to SC21/SWG-PS, SGFS, December 1993
SGFS N 1089	White Paper on OSE Profiling Concepts, SGFS, December 1993 (material offered for integration in ISO/IEC TR 10000)
SGFS N 1090	Liaison Statement to JTC1 on the Subject of PAS and APIs, December 1993
SGFS N 1099	Draft Minutes of the SGFS Authorized Subgroup Meeting in Amsterdam, 29 November to 3 December 1993, SGFS, December 1993
SGFS N 1098	Resolutions Adopted by the SGFS Authorized Subgroup Meeting in Amsterdam, 29 November to 3 December 1993, SGFS, December 1993
Other Documents—SC6	
SC6 N 8135	Draft Statement of Expected Benefits Regarding Category C Liaison Between the Internet Society and ISO/IEC JTC1/SC6, July 1993

SC6 N 8419	ISO/IEC JTC1/SC6 Liaison Contribution to the Internet Society, November 1993
SC6 N 8420	Statement of Expected Benefits Resulting from Liaison Between ISO/IEC JTC1/SC6 and the Internet Society, November 1993
Other Documents—SC21	
SC21 N 5194	Resolutions of the Fourth Plenary Meeting of SC21, 5 June 1990, Seoul
SC21 N 5228	Report of the ISO/IEC JTC1/SC21 Plenary Meeting, 5 June 1990, Seoul, Korea
SC21 N 5229	Report of the JTC1/SC21 Plenary Meeting, 5 June 1990, Seoul, Republic of Korea
SC21 N 5714	Resolutions of the ISO/IEC JTC1 Advisory Group Meeting, Washington, DC., 19-21 February 1991
SC21 N 6273	Resolutions of the Seventh Plenary Meeting of ISO/IEC JTC1/SC21, 4-5 June 1991, Arles, France
SC21 N 6478	Target Dates for Completion of SC22 Projects
SC21 N 6527	Resolutions of the ISO/IEC JTC1 Plenary Meeting, October 2-4, 1991, Madrid, JTC1 Secretariat
SC21 N 6530	Report of the JTC1 Plenary Ad Hoc Group on EDI
SC21 N 6606	Collection of Liaison Statements from SC27 to SC21
SC21 N 6615	The Processing of Standards in SC21, SC21 Special Meeting on Structure and Organization
SC21 N 6619	Resolutions of the SC21 Special Meeting on Structure and Organization, ANSI
SC21 N 6711	SC21 SD-4, SC21 Strategic Plan
SC21 N 6713	ITU-TS Circular No. 118 Regarding the Catalogue of CCITT Recommendations
SC21 N 6714	List of Contact Points of SIGs/EGs of Regional Workshops
SC21 N 6715	Letter from ITTF/ITU-TS Regarding Preparation of CCITT-ISO/IEC Common Text
SC21 N 6777	Letter from ISO Regarding the Disbandment of GOST
SC21 N 6778	ITU-TS Interim Meeting Schedule
SC21 N 6779	Statement Regarding Participation at CCITT Study Group Meetings
SC21 N 6807	Protocol Version Numbers
SC21 N 6883	Report of the Secretariat to the SC21 Meeting in Ottawa
SC21 N 6905	Liaison Statement to SC21/WG6: Report on Q26/VII Meeting
SC21 N 6907	Liaison Statement to SC21 Concerning Collaborative Work on ODP, Security, ASN.1, ROSE, and RTSE
SC21 N 6943	Requirements and Recommendations Regarding Protocol Version Numbers
SC21 N 6943 Rev	Requirements and Proposed Recommendations of the Protocol Version Numbers Pre-Meeting (and the Initial ITTF Response)
SC21 N 6957	Project Dependencies
SC21 N 6966	Incorporation of Versions and Extensibility Technical Material into Existing Standards and Other Documents
SC21 N 6969	Comments on SC21 N 6943, Recommendations and Requirements on Protocol Version Numbers
SC21 N 7099	Resolutions Approved by SC21/WG1 at Its Ottawa Meeting
SC21 N 7101	List of Late Input Documents and Output Documents of the SC21/WG1 Ottawa Meeting
SC21 N 7132	Request for National Body Comment on NWI for Library/Catalogue
SC21 N 7140	Reply to Liaison Statement for CCITT SG VII Regarding the Comments on Notational Tools in SC21 N 6568, 9 July 1992
SC21 N 7195	SC21 Position on SC21 N 6484 "Guide for CCITT and JTC1 Collaboration"
SC21 N 7196	SC21 SD- 8, SC21 Schedule of Meetings SC21 Plenary Meeting
SC21 N 7204 Rev	Resolutions of the Eight Plenary Meeting of ISO/IEC JTC1/SC21, Revised
SC21 N 7205	ISO/IEC JTC1/SC21 Programme of Work
SC21 N 7206	WG3 Recommendations, ISO/IEC JTC1/SC21/WG3, Ottawa
SC21 N 7214	Rapporteur's Report on SC21 Strategic Planning
SC21 N 7215	Revised Management Guidelines for ISO/IEC JTC1/SC21
SC21 N 7268	Collection of Definitions of OSI Vocabulary
SC21 N 7375	Call for Contributions on SC21/WG4 Title and Terms of Reference
SC21 N 7379	Liaison Statement to SC21 on OSI Profile Conformance Requirements in TR 10000-1
SC21 N 7713	Resolutions of the ISO/IEC JTC1 Plenary Meeting, 23-26 March 1993, Berlin, Germany
SC21 N 7720	Revised Title and Scope for SC21
SC21 N 7728	Proposals for Re-assessment or Cancellation of Specific SC21 Projects
SC21 N 7747	Revised Text of the Guide for CCITT and ISO/IEC JTC1 Cooperation
SC21 N 7749	The International Telecommunication Union - An Overview
SC21 N 7841	Report of the Ninth Plenary Meeting of ISO/IEC JTC1/SC21 to be held from 29-30 June 1993 in Yokohama, Japan
SC21 N 7915	Liaison Statement to SC6 in Reply to SC6 N 7961 and 7614, SC21/WG8, August 1993
SC21 N 7983	Liaison Statement to SC21/WG8 and SC27 on Future Liaison Activity, SC21/WG4, August 1993
SC21 N 8103 Rev.	Request from SC21 to JTC1 Concerning the "Fast Tracking" of the PCTE Document, June 1993
SC21 N 8122	Management Guidelines
SC21 N 8034	Liaison Statement to the Object Management Group, SC21/WG7, August 1993

SC21 N 8081	Resolutions of the Ninth Plenary Meeting of ISO/IEC JTC1/SC 21, 29-30 June 1993, Yokohama, Japan
SC21 N 8128	Liaison Statement to the Internet Society, SC21, June 1993
SC21 N 8129	Statement of Benefits on Establishment of C-Liaison with X/Open, SC21, June 1993
SC21 N 8130	Statement of Benefits on Establishment of C-Liaison with the Object Management Group (OMG), SC21, June 1993
SC21 N 8131	Statement of Benefits on Establishment of C-Liaison with the Internet Society, SC21, June 1993
SC21 N 8193	Status of X.Series Recommendations, ITU-TS SG7, August 1993
SC21 N 8251	Proposed Approval of 27 Recommendations Agreed to by Study Group 7 at its Meeting on 2 July 1993, ITU-TS, October 1993
SC21 N 8261	Liaison Between SC24 and SC21, SC24, October 1993
SC21 N 8318	Establishment of Formal Liaison Between JTC1/SC21 and JTC1/SC29, SC29, December 1993
SC21/WG6 N 1152	Proposals for Changes to SC21/WG6 Programme of Work

C. FORMAL DESCRIPTION TECHNIQUES (FDTs):

ISO 8807	LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour (Z.100)
	AM[10] 1 — Graphical Representation of LOTOS (G-LOTOS)
	WDAM 2 — Enhancements to LOTOS
ISO 9074	Estelle - A Formal Description Technique Based on an Extended State Transition Model
	AM 1 — Estelle Tutorial
WD 9074.2[11]	Estelle - A Formal Description Technique Based on an Extended State Transition Model, Edition 2 (incorporates AM 1)
ISO/TR 10167◆	Guidelines for the Application of Estelle, LOTOS, and SDL (Z.110)
PDTR 11589	LOTOS Description of the CCR Service, 1993
PDTR 11590	LOTOS Description of the CCR Protocol, 1993
SC21 N 6088	Proposal for a WG7 Question on the Suitability of the Formal Description Technique Z for Use in ODP
SC21 N 7096	Draft Answer to Q1/48.6 - G-LOTOS
SC21 N 8022	NP on Enhancements to LOTOS
SC21 N 8023	Initial Draft on Enhancements to LOTOS, SC21/WG1, November 1993
SC21 N 8122	Update to Management *Guidelines* on Formal Descriptions, SC21, June 1993
SC21 N 8280	Liaison Statement to SC21/WG4 on Requirements and Directions for the Use of Formal Description Techniques for the Specification of Managed Objects, ITU-TS SG7, October 1993
SC21/WG1 N 1157	Contributions on LOTOS Enhancements
ITU-TS Z.100 Rev 1	Specification and Description Language (SDL)
ITU-TS Z.110	Criteria for the Use and Applicability of Formal Description Techniques
ITU-TS Z.120	Messages Sequence Charts

D. SECURITY:

Interconnection Standards for Security:

ISO 8372	Modes of Operation for a 64-bit Block Cipher Algorithm
ISO/IEC 9160	Physical Layer Interoperability Requirements
ISO/IEC 9796	Digital Signature Scheme Giving Message Recovery
ISO/IEC 9797	Data Integrity Mechanisms Using a Cryptographic Check Function Employing a Block Cipher Algorithm
ISO/IEC 9798-1	Security Techniques - Entity Authentication Mechanisms, Part 1: General Model
DIS 9798-2	Security Techniques - Entity Authentication Mechanisms, Part 2: Entity Authentication Using Symmetric Techniques, SC27/WG2, 1993
DIS 9798-3	Security Techniques - Entity Authentication Mechanisms, Part 3: Entity Authentication Using a Public Key Algorithm, SC27/WG2, 1993
WD 9798-4	Security Techniques - Entity Authentication Mechanisms, Part 4: Entity Authentication Using Non-Reversible Functions, SC27/WG2, 1993
WD 9798-x	Security Techniques - Entity Authentication Mechanisms, Part x: Entity Authentication Using Zero-Knowledge Techniques, SC27/WG2, 1993
ISO 9979	Procedures for the Registration of Cryptographic Algorithms
ISO/IEC 10116	Modes of Operation for an N-bit Block Cipher Algorithm

---

10 AM: Amendment to ISO standard.

11 For ISO standards, the decimal indicates the version number; thus, WD 9074.2 is Version 2 (no decimal indicates Version 1).

DIS 10118-1	Security Techniques - Hash Functions, Part 1: General Model, SC27/WG2, 1993
DIS 10118-2	Security Techniques - Hash Functions, Part 2: Hashing Operation Using Symmetric Block-Cypher Algorithm, SC27/WG2, 1993
WD 10118-3	Security Techniques - Hash Functions, Part 3: Dedicated Hash Functions, SC27/WG2, SC27 N 223, 1993
WD 10118-4	*Security Techniques - Hash Functions, Part 4:* **Hash Functions Using Modular Arithmetic,** SC27/WG2 N 21, 1993
CD[12] 10181-1.2◆	Security Frameworks in Open Systems, Part 1: Overview
ISO/IEC 10181-2◆	Security Frameworks in Open Systems, Part 2: Authentication Framework (passed DIS ballot in October 1993)
	WDAM[13] 1 Authentication Elements
DIS[14] 10181-3◆	Security Frameworks in Open Systems, Part 3: Access Control Framework
DIS 10181-4◆	Security Frameworks in Open Systems, Part 4: Non-Repudiation Framework
DIS 10181-5◆	Security Frameworks in Open Systems, Part 5: Confidentiality Framework
DIS 10181-6◆	Security Frameworks in Open Systems, Part 6: Integrity Framework
CD 10181-7.2◆	Security Frameworks in Open Systems, Part 7: Security Audit Framework
W[15] 10181-8	Security Frameworks in Open Systems, Part 8: Key Management
ISO/IEC 10736	Transport Layer Security Protocol, October 1993
	PDAM[16]1 Security Association Establishment Protocol
ISO/IEC 10745◆	Upper Layer Security Model
DIS 11577◆	Network Layer Security Protocol
DIS 11586-1	Generic Upper Layers Security (GULS), Part 1: Overview, Models and Notation (X.830)
DIS 11586-2	Generic Upper Layers Security (GULS), Part 2: Security Exchange Service Element (SESE) Service Definition (X.831)
DIS 11586-3	Generic Upper Layers Security (GULS), Part 3: Security Exchange Service Element (SESE) Protocol Specification (X.832)
DIS 11586-4	Generic Upper Layers Security (GULS), Part 4: Protecting Transfer Syntax Specification (X.833)
WD 11586-5	Generic Upper Layers Security (GULS), Part 5: PICS Proforma (X.834)
WD 11586-6	Generic Upper Layers Security (GULS), Part 6: Protecting Transfer Syntax - PICS Proforma (X.835)
WD 11770-1	Key Management, Part 1: Framework
CD 11770-2	Key Management, Part 2: Key Management Mechanisms Using Symmetric Techniques
CD 11770-3	*Key Management, Part 3: Key Management Mechanisms Using Asymmetric Techniques*
PDTR 13335-1	Security Techniques - Guidelines for Management of Information Technology Security, Part 1: Concepts and Models, SC27/WG1, 1993
WDTR 13335-2	Security Techniques - Guidelines for Management of Information Technology Security, Part 2: Managing and Planning, SC27/WG1, 1993
WDTR 13335-3	Security Techniques - Guidelines for Management of Information Technology Security, Part 3: Techniques, SC27/WG1, 1993
ITU-TS X.800	Security Architecture for Open Systems Interconnection for CCITT Applications (ISO 7498-2), 1991
ITU-TS X.802	Lower Layers Security Model (TR 13594), Draft, 1993
ITU-TS X.810	Security Frameworks in Open Systems: Security Authentication Frameworks Overview (ISO 18181-1), Draft, 1993
ITU-TS X.811	Security Frameworks in Open Systems: Authentication Framework (ISO 18181-2), Draft, 1993
ITU-TS X.812	Security Frameworks in Open Systems: Access Control Framework (ISO 18181-3), Draft, 1993
ITU-TS X.813	Security Frameworks in Open Systems: Non-Repudiation Framework (ISO 18181-4), Draft, 1993
ITU-TS X.814	Security Frameworks in Open Systems: Confidentiality Framework (ISO 18181-5), Draft, 1993
ITU-TS X.815	Security Frameworks in Open Systems: Integrity Framework (ISO 18181-6), Draft, 1993
ITU-TS X.816	Security Frameworks in Open Systems: Security Audit Framework (ISO 18181-7), Draft, 1993
ITU-TS X.830	Generic Upper Layers Security - Security Eexchange Service Element: Overview, Model and notation (ISO 11586-1), Draft, 1993
ITU-TS X.831	Generic Upper Layers Security: Security Eexchange Service Element (SESE) Service Definition (ISO 11586-2), Draft, 1993
ITU-TS X.832	Generic Upper Layers Security: Security Eexchange Service Element (SESE) Protocol Specification (ISO 11586-3), Draft, 1993

12 CD: Committee Draft for ISO standard [formerly Draft Proposal (DP)].

13 WDAM: Working Draft Amendment to an ISO Standard (has the status of a WD).

14 DIS: Draft International Standard for ISO.

15 WD: Working Draft for ISO (status of text prior to being submitted as a Committee Draft).

16 PDAM: Proposed Draft Amendment to an ISO Standard (has the status of a CD).

ITU-TS X.833	Generic Upper Layers Security: Protecting Transfe Syntax Specification (ISO 11586-4), Draft, 1993
ITU-TS X.834	Generic Upper Layers Security: Security Eexchange Service Element (SESE) PICS Proforma (ISO 11586-5), Draft, 1993
ITU-TS X.835	Generic Upper Layers Security: Security Eexchange Service Element (SESE) Protecting Transfer Syntax PICS Proforma (ISO 11586-6), Draft, 1993
Other Security Standards:	
ISO 7816-1	Identification Cards - Identification Cards with Contacts, Part 1: Physical Characteristics, SC17/WG4
ISO 7816-2	Identification Cards - Identification Cards with Contacts, Part 2: Number and Position of Contacts, SC17/WG4
ISO 7816-3	Identification Cards - Identification Cards with Contacts, Part 3: Electronic Signals/Exchange Protocols, SC17/WG4
ISO 8730	Financial Transactions - Wholesale Banking Security - Requirements for Message Authentication, TC68/SC2
ISO 8731-1	Financial Transactions - Wholesale Banking Security - Approved Algorithms for Message Authentication, Part 1: DEA-1 Algorithm, TC68/SC2
ISO 8731-2	Financial Transactions - Wholesale Banking Security - Approved Algorithms for Message Authentication, Part 2: Message Authenication Algorithm, TC68/SC2
ISO 8732	Financial Transactions - Wholesale Banking Security - Key Management, TC68/SC6
ISO 9807	Financial Transactions - Retail Banking Security - Requirements for Message Authentication, TC68/SC6/WG6
ISO 9564-1	Financial Transactions - Retail Banking Security - Personal Identification Number (PIN) Management and Security, Part 1: PIN Protection Principles and Techniques, TC68/SC6/WG6
ISO 9564-2	Financial Transactions - Retail Banking Security - Personal Identification Number (PIN) Management and Security, Part 2: Approved Algorithms for PIN Encipherment, TC68/SC6/WG6
ISO/IEC 10126-1	Financial Transactions - Wholesale Banking Security - Procedures for Message Encipherment, Part 1: General Principles, TC68/SC2, 1993
ISO/IEC 10126-2	Financial Transactions - Wholesale Banking Security - Procedures for Message Encipherment, Part 2: DEA- Algorithms, TC68/SC2, 1993
DIS 10175	Text and Office Systems - Document Printing Applicaion (DPA), SC18/WG4
ISO/IEC 10202-1	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Card Life Cycle TC68/SC6/WG7, 1993
DIS 10202-2	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Transaction Process, TC68/SC6/WG7, 1993
CD 10202-3	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Cryptographic Key Relationship, TC68/SC6/WG7, 1993
ISO/IEC 10202-4	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Secure Application Modules, TC68/SC6/WG7, 1993
CD 10202-5	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Use of Algorithms, TC68/SC6/WG7, 1993
DIS 10202-6	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Cardholder Verification, TC68/SC6/WG7, 1993
WD 10202-7	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Key Management, TC68/SC6/WG7, 1993
DIS 11568-1	Financial Transactions - Retail Banking Security - Key Management, Part 1: Introduction to Key Management, TC68/SC6/WG6, 1993
ISO/IEC 11131	Financial Transactions - Wholesale Banking Security - Sign-On Authemtication, TC68/SC2, 1993
DIS 11166-1	Financial Transactions - Wholesale Banking Security - Key Management by Means of Asymmetric Algorithms, Part 1: Principles, Procedures, and Formats, TC68/SC2, 1993
DIS 11166-2	Financial Transactions - Wholesale Banking Security - Key Management by Means of Asymmetric Algorithms, Part 2: Approved Algorithms Using RSA Cryptosystem, TC68/SC2, 1993
DIS 11568-1	Financial Transactions - Retail Banking Security - Key Management, Part 1: Introduction to Key Management, TC68/SC6/WG6, 1993
DIS 11568-2	Financial Transactions - Retail Banking Security - Key Management, Part 2: Key Management Techniques for Symmetric Ciphers, TC68/SC6/WG6, 1993
DIS 11568-3	Financial Transactions - Retail Banking Security - Key Management, Part 3: Key Life Cycle for Symmetric Ciphers, TC68/SC6/WG6, 1993
WD 11568-5	Financial Transactions - Retail Banking Security - Key Management, Part 5: Key Management Techniques for Asymmetric Ciphers, TC68/SC6/WG6, 1993
WD 11568-6	Financial Transactions - Retail Banking Security - Key Management, Part 6: Key Life Cycle for Asymmetric Ciphers, TC68/SC6/WG6, 1993
WD 11568-7	Financial Transactions - Retail Banking Security - Key Management, Part 7: Key Management Schemes, TC68/SC6/WG6, 1993

CD 11568-8	Financial Transactions - Retail Banking Security - Key Management, Part 8: Key Managementg Related Data Elements, TC68/SC6/WG6, 1993
WD 13182	Financial Transactions - Security Architecture - System Overview, TC68/SC6/WG7, 1993
CD 13492	Financial Transactions - Retail Banking Security - Secure Cryptographic Devices, TC68/SC6/WG6, 1993
Working Papers on Security:	
SC6 N 7951	OSI Lower Layer Security Model, SC6/WG5, 1993
SC6 N 7952	Lower Layer Security Guidelines, SC6/WG5, 1993
SC18 N 2233	User Requirements for Security in Text and Office Systems
SC21 N 8020	Liaison Statement to JTC1/SC27 on Open Systems Security, SC21/WG1, August 1993
SC21 N 8269	Liaison Statement to SC21 WG/8 on Security Activities, ITU-TS SG7, October 1993
SC21 N 8325	Authentication and Privilege Attribute Security Application with Related Key Distribution Functions, Part 1: Overview and Functional Model, ECMA/TC-TG9, November 1993
SC21 N 8326	Authentication and Privilege Attribute Security Application with Related Key Distribution Functions, Part 2: Security Information Objects, ECMA/TC-TG9, November 1993
SC21 N 8327	Authentication and Privilege Attribute Security Application with Related Key Distribution Functions, Part 3: Service Definitions, ECMA/TC-TG9, November 1993
SC21 N 8328	Liaison Statement to SC21/WG8 Regarding Authentication and Related Security Services for Distributed Applications, ECMA/TC-TG9, November 1993
SC21 N 8329	Liaison Contribution to SC21/WG8 Regarding Authentication and Related Security Services for Distributed Applications - Extended Schematic for First Draft, ECMA/TC-TG9, November 1993
SC21 N 8380	Guide to Open System Security, Working Draft Technical Report, December 1993
SC21 N 3283	Working Draft for Lower-Layer Security Model
SC21 N 4833	Report to JTC1 from SC27 on Security Techniques, SC27 Secretariat
SC21 N 4835	Report of the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990, SC27 Secretariat
SC21 N 4836	Resolutions Taken at the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990
SC21 N 5580	New Area of Work for SC27/WG1 on IT Security Information Objects
SC21 N 5581	New Area of Work for SC27/WG1 on IT Security Terminology
SC21 N 5731	Progression of the Upper Layers Security Standards, Canada
SC21 N 6586	Meeting Report - Collaborative CCITT Q19/VII and SC21/WG6 Meeting on Upper Layers Security
SC21 N 6695	Liaison Statement from SC21/WG1 Security Ad Hoc Group to SC21/WG5 TP on Preliminary Security Model
SC21 N 6656	Liaison Statement to SC21/WG6 on Compatibility of ROS and RPC
SC21 N 6755	Contribution on Key Management
SC21 N 6765	Guide to Open Systems Security Collaborative SC21/ITU-TS Security Ad Hoc Group Meeting
SC21 N 6843	Contribution on Non-Repudiation Framework
SC21 N 6844	Contribution on Security Frameworks Overview
SC21 N 6875	Liaison Statement to SC21 from SC18 on "Revised Draft Guide to Open Systems Security"
SC21 N 6877	Liaison Statement to SC21 from SC18 on Security Framework SC18
SC21 N 6878	Liaison Statement to CCITT Q19/VII and SC21/WG6 from SC18 on Use of the Security Exchange ASE
SC21 N 6893	Liaison Statement to SC21 on Approval of Management Framework
SC21 N 6974	Liaison Statement to SC6 Concerning a Request for Incorporation of New Protocol Information Attributes in ISO/IEC 9594-6/DAM 1
SC21 N 6996	Liaison Statement to SC6 on Common Aspects of OSI Upper/Lower Layer Security Standards
SC21 N 6997	Liaison Statement to ECMA on Security in the Upper Layers
SC21 N 6998	Authentication and Related Security Services for Distributed Applications
SC21 N 7086	Liaison Statement to SC18 on Security
SC21 N 7087	Liaison Statement to SC27 on Security
SC21 N 7089	Statement on Scope and Usability of the Open Systems Security Framework
SC21 N 7098	Proposed New Question Q1/69 on Conformance Assessments for OSI Security
SC21 N 7134	Preliminary Document on Multiple Input Metric Object
SC21 N 7145	Liaison Statement to SC21/WG1, SC21/WG6 (8), SC6 and SC27 on Security Requirements for Systems Management
SC21 N 7149	Liaison Statement to SC18 Regarding the Status of the Security Exchange Work
SC21 N 7292	Guide for Open Systems Security
SC21 N 7914	Working Document on Authentication and Related Security Services
SC21 N 8330	Version V2 of the APA-Application Standard, ECMA/TC-TG9, November 1993 (standard has three parts: Overview and Functional Model, Security Information Objects, and Service Definitions)
SC21 N 8380	Guide to Open Systems Security
SC21/WG6 N 1123	UK Position on Alignment of Upper and Lower Layer Security Protocols
SC21/WG6 N 1124	UK Comment on SC21 N 6130, Generic Transfer Syntax Providing Upper Layers Security
SC21/WG6 N 1158	Strawman Generic Security ESO-OSI Abstract Interface

SC21/WG8 N 173	Authentication and Related Security Services, Part 2: Generic Abstract Services for Security (GASS), Strawman
SC22/WG15 N 46 Rev.	Security Interface for POSIX, SC22/WG15, 1993 (approved new work item)
SC27 N 209	Non-Repudiation Mechanisms (Part 1: General Model; Part 2: Mechanisms Using Symmetric Key Techniques; and Part 3: Mechanisms Using Asymmetric Techniques), SC27/WG2
SC27 N 467	Collection and Analysis of Requirements for Information Technology Security Criteria, SC27/WG3
SC27 N 685	Security Information Objects, SC27/WG1, 1993
SC27 N 691	Guidelines on the Use and Selection of Security Services and Mechanisms for the Management of Trusted Third Party Services, SC27/WG1, 1993
SC27 N 697	Glossary of Information Technology Security Definitions, SC27/WG1, 1993 (SC27 standing document)
SC27 N 718	Evaluation Criteria for Information Technology Security, Part 2: Introduction and Model, SC27/WG3, 1993
SC27 N 721	Evaluation Criteria for Information Technology Security, Part 3: Functionality of IT Systems, SC27/WG3, 1993
SC27 N 734	Evaluation Criteria for Information Technology Security, Part 1: Assurance of IT Systems, SC27/WG3, 1993
SC27 N 791	Security Incident Reporting; WG1 Meeting No. 7; 12-15 October 1993 in Paris, SC27/WG1, November 1993

E. OSI MANAGEMENT:

STANAG 4407◆	System Management, Draft, NATO UNCLASSIFIED (cf. ISO 10165-1, 10165-2, 10165-4, 10164, 11183, 12059, 12060)	
	Main Body, Preliminary Draft	
	Annex A—Security of Management (under development)	
	Annex B—Military Features, Preliminary Draft	
	Annex C—The Development of NSPs for Systems Management, Preliminary Draft	
	Annex D—NSP zzzz: Basic Systems Management, Preliminary Draft (STANAG 4407-1)	
ISO/IEC 9595◆	Common Management Information Service (CMIS) Definition (X.710:1991)	
	DAM 3	Support of Allomorphism
	AM 4	Access Control
	WDAM 5	Enhanced Functionality
	Cor 1-2	Technical Corrigenda 1-2
ISO/IEC 9596-1	Common Management Information Protocol (CMIP) Specification (X.711:1991)	
	PDAM 3	Support of Allomorphism
	PDAM 4	State Table[17]
	WDAM 5	Enhanced Functionality
	Cor 1-4	Technical Corrigenda 1-4
ISO/IEC 9596-2	Common Management Information Protocol (CMIP) Specification, Part 2: PICS Proforma (X.712)	
	Cor 1	Technical Corrigendum 1
ISO/IEC 10040◆	Systems Management Overview (X.701)	
	AM 1	Management Knowledge Management Architecture
	PDAM 2	Management Domains Architecture
	Cor 1	Draft Technical Corrigendum 1
ISO/IEC 10164-1◆	Systems Management, Part 1: Object Management Function (X.730)	
	DAM[18] 1	ICS Proforma
ISO/IEC 10164-2◆	Systems Management, Part 2: State Management Function (X.731)	
	DAM 1	ICS Proforma
ISO/IEC 10164-3◆	Systems Management, Part 3: Attributes for Representing Relationship (X.732)	
	DAM 1	ICS Proforma
ISO/IEC 10164-4◆	Systems Management, Part 4: Alarm Reporting Function (X.733)	
	DAM 1	ICS Proforma
ISO/IEC 10164-5◆	Systems Management, Part 5: Event Report Management Function (X.734)	
	DAM 1	ICS Proforma
	PDAM 2	Enhanced Discriminator
ISO/IEC 10164-6◆	Systems Management, Part 6: Log Control Function (X.735)	
	DAM 1	ICS Proforma
	PDAM 2	Enhanced Log

[17] Work on a PDAM for State Table to ISO 9596-1 was cancelled in June 1991.

[18] DAM: Draft Amendment for an ISO standard (has the status of a DIS).

ISO/IEC 10164-7•	Systems Management, Part 7: Security Alarm Reporting Function (X.736)
	DAM 1 ICS Proforma
ISO/IEC 10164-8•	Systems Management, Part 8: Security Audit Trail Function (X.740)
	Cor 1 Technical Corrigendum 1, January 1994
ISO/IEC 10164-9•	Systems Management, Part 9: Objects and Attributes for Access Control
DIS 10164-10.2	Systems Management, Part 10: Usage Metering Function (X.742)
	WDAM 1 ICS Proforma
ISO/IEC 10164-11•	Systems Management, Part 11: Metric Objects and Attributes (X.739)
	WDAM 1 ICS Proforma
	WDAM 2 Additional Metric Objects and Attributes
ISO/IEC 10164-12•	Systems Management, Part 12: Test Management Function (X.745)
	PDAM 1 ICS Proforma
ISO/IEC 10164-13•	Systems Management, Part 13: Measurement Summarization Function (X.738)
	WDAM 1 ICS Proforma
	WDAM 2 Additional Summarization Scanners
DIS 10164-14.2	Systems Management, Part 14: Confidence and Diagnostic Test Categories
DIS 10164-15	Systems Management, Part 15: Scheduling Function
CD 10164-16.2	Systems Management, Part 16: Working Document on Management Knowledge Management
CD 10164-17	Systems Management, Part 17: Change Over Function
	WDAM 1 General Relationship Model
CD 10164-19	Systems Management, Part 19: Management Domain and Management Policy Management Function
WD 10164-ev.2	Systems Management, Part ev: Enhanced Event Control Function
WD 10164-mo	Systems Management, Part mo: Managed Objects for Supporting Upper Layers, January 1994
WD 10164-rm.2	Systems Management, Part rm: General Relationship Management Function
WD 10164-rtm	Systems Management, Part rtm: Response Time Monitoring Function
WD 10164-sw	Systems Management, Part sw: Software Management Function
WD 10164-tm.2	Systems Management, Part tm: Time Management Function
ISO/IEC 10165-1•	Structure of Management Information, Part 1: Management Information Model (X.720)
	PDAM 1 Generalization of Terms
	Cor 1 Technical Corrigendum
ISO/IEC 10165-2•	Structure of Management Information, Part 2: Definition of Management Information (X.721)
	PDAM 1 Enhanced Discriminator and Log
	Cor 1 Draft Technical Corrigendum
ISO/IEC 10165-4•	Structure of Management Information, Part 4: Guidelines for the Definition of Managed Objects (X.722)
	PDAM 1 GDMO Extensions
	PDAM 2 Set By Create and Component Registration
ISO/IEC 10165-5•	Structure of Management Information, Part 5: Generic Management Information (X.723)
ISO/IEC 10165-6•	Structure of Management Information, Part 6: Requirements and Guidelines for Management Information Conformance Statement (MICS) Proformas (X.724)
	WDAM 1 Manager Role Conformance
	Cor 1 Draft Technical Corrigendum, January 1994
WD 10165-7.2•	Structure of Management Information, Part 7: Management Information Register and Registration Procedures
WD 10165-x	Structure of Management Information, Part x: Management Information in the Upper Layers
ISO/IEC 10733	Elements of Management Information Related to OSI Network Layer Standards
DIS 10742	Specification of the Elements of Management Information Related to OSI Data Link Layer Standards, 1993
SGFS N 1076	Liaison from AOW/EWOS/OIW to SGFS on Submission of AOM 2x Taxonomy, SGFS, December 1993
SC21 N 4077	Fault Management Working Document
SC21 N 4085	Accounting Management Working Document
SC21 N 4091	OSI Security Management Working Document
SC21 N 4970	Systems Management Tutorial - Annex A: Access Control
SC21 N 6037	Need for Security Services with OSI Management
SC21 N 6194	Final Answer to Q1/63.1--Meaning of Conformance to Objects in the Context of OSI Management
SC21 N 6306	Performance Management Working Document
SC21 N 6799	Contribution on Upper Layer Management
SC21 N 6870	Proposal for a New Work Item on Mapping of the OSI System Management - Object Management Function onto Message Oriented Text Interchange System (MOTIS)

SC21 N 6914	Liaison Statement to SC21: Request for Review & Comment on Profile Choices for Subclasses of the EFD/LOG Managed Object Classes Using Allomorphism & Best Efforts Management EWOS for Regional Workshop Network Management Coordination Com.
SC21 N 6915	Liaison Statement to SC21 Regarding Profiles for Systems Management Functions
SC21 N 6968	Request for Comment on Issues Concerning Upper Layer Management
SC21 N 7091	Liaison Statements to SC18 on Quality of Service
SC21 N 7105	Reply and Disposition of Comments on NP on Development of Enhanced Functionality for CMIS/P (JTC1 N 1667), ISO/IEC JTC1/SC21/WG4 Meeting
SC21 N 7106	Agreed Requirements for Enhanced Functionality for SM Communications
SC21 N 7107	NP on Disposition of Ballot Comments on JTC1 N 1439, Proposal for an Enhanced Event Handling & Log Control
SC21 N 7109	Command Sequencer for Systems Management
SC21 N 7117	Request for National Body Input on Principles of Conformance for Managing Systems
SC21 N 7118	Management Domains Architecture
SC21 N 7119	Management Domain Management Function
SC21 N 7122	Working Draft on Application Context for Systems Management with TP
SC21 N 7126	General Relationship Model--Third Working Draft
SC21 N 7129	Request for National Body Contributions to Progress Work on Distributed Management
SC21 N 7131	Request for National Body Input Regarding Definition of Common Terms and Use of Formal Description Techniques in SMI Standards
SC21 N 7132	Preliminary Document on Multiple Input Metric Object
SC21 N 7133	Coherence of Extended Management Architecture
SC21 N 7134	Request for National Body Comment on NP for Library/Catalog
SC21 N 7135	Call for Contributions on Priority Mechanisms in Systems Management
SC21 N 7146	Liaison Statement to SC22/WG15 on Software Management
SC21 N 7147	Liaison Statement to CCITT Q23/IV on Software MO
SC21 N 7148	Response to the SC6 Liaison Statement on Event Definition
SC21 N 7483	Proposal for a New Work Item on Mapping of OSI System Management - Object Management Function onto Message Handling Service (MHS)
SC21 N 7955	SC21/WG4 Standing Document 1: Issues for Extended Systems Management Architecture, July 1993
SC21 N 7957	Extended Systems Management Architecture
SC21 N 7959	Expiry Behavior
SC21 N 7962	Working Document for Command Sequencer for Systems Management
SC21 N 7965	Definition of Systems Management Protocol Machine Managed Objects
SC21 N 7970	Enhanced Functionality for Systems Management Communications
SC21 N 7980	Liaison Statement to ITU-TS/SG15 on Change Over Function, August 1993
SC21 N 8037	Issues for Management Domain Management Function
SC21 N 8040	Relationship Management Function, Second Working Document
SC21 N 8161	Working Draft on Enhancements to Metric Objects and Attributes, SC21/WG4, July 1993
SC21 N 8162	Working Draft for ICS Proforma for Metric Objects and Attributes, SC21/WG4, July 1993
SC21 N 8163	Working Draft for ICS Proforma for Summarization Function, SC21/WG4, July 1993
SC21 N 8178	Working Document on Managed Objects for Upper Layers
SC21 N 8281	Liaison Statement to SC21/WG4 Concerning the OSI Systems Management Implementor's Guide, ITU-TS SG7, October 1993
SC21/WG4 N 1472	US Response to SC21 N 6679, Request for National Body Comments on the Progression of an Amendment to ISO/IEC 10164-11 on the Definition of Multiple Input Metric Objects
SC21/WG4 N 1438	UK Contribution to 21/63.2, Testability of Managed Objects
SC21/WG4 N 1641	Issues for Extended Systems Management Architecture (WG4 SD 1)
SC21/WG4 N 1831	Second Working Draft on Expiry Behavior, December 1993
SC21/WG4 N 1832	Command Sequencer, Working Draft, December 1993
SC21/WG4 N 1853	Manager Role Conformance, Second Working Draft, December 1993
ITU-TS X.700	Management Framework for Open Systems Interconnection (OSI) for CCITT Applications (ISO 7498-4), 1992
ITU-TS X.701	Systems Management Overview (ISO 10040), 1992
ITU-TS X.702	Application Context for Systems Management for Transaction Processing (ISO 11587), Draft, 1993
ITU-TS X.710	Common Management Information Service Definition for CCITT Applications(ISO 9595), 1991
ITU-TS X.711	Common Management Information Protocol Specification for CCITT Applications (ISO 9596-1), 1991
ITU-TS X.712	Common Management Information Protocol: PICS Proforma (ISO 9596-2), 1992
ITU-TS X.720	Structure of Management Information: Management Information Model (ISO 10165-1), 1992
ITU-TS X.721	Structure of Management Information: Definition of Management Information (ISO 10165-2), 1992

ITU-TS X.722	Structure of Management Information: Guidelines for the Definition of Managed Objects (ISO 10165-4), 1992
ITU-TS X.723	Structure of Management Information - Generic Management Information (ISO 10165-5), Draft, 1993
ITU-TS X.724	Structure of Management Information - Requirements and Guidelines for Implementation of Conformance Statement Proformas Associated with Management Information (ISO 10165-6), Draft, 1993
ITU-TS X.725	Structure of Management Information - General Relationship Model (ISO 10165-7), Draft, 1993
ITU-TS X.730	Systems Management: Object Management Function (ISO 10164-1), 1992
ITU-TS X.731	Systems Management: State Management Function ISO 10164-2), 1992
ITU-TS X.732	Systems Management: Attributes for Representing Relationships (ISO 10164-3), 1992
ITU-TS X.733	Systems Management: Alarm Reporting Function (ISO 10164-4), 1992
ITU-TS X.734	Systems Management: Event Report Management Function (ISO 10164-5), 1992
ITU-TS X.735	Systems Management: Log Control Function (ISO 10164-6), 1992
ITU-TS X.736	Systems Management: Security Alarm Report Function (ISO 10164-7), 1992
ITU-TS X.737	Systems Management: Confidence and Diagnosic Test Categories (ISO 10164-14), Draft, 1993
ITU-TS X.738	Systems Management: Summarization Function (ISO 10164-13), Draft, 1993
ITU-TS X.739	Systems Management: Metric Objects and Attributes (ISO 10164-11), Draft, 1993
ITU-TS X.740	Systems Management: Security Audit Trail Function (ISO 10164-8), Draft, 1993
ITU-TS X.741	Systems Management: Objects and Attributes for Access Control (ISO 10164-9), Draft, 1993
ITU-TS X.742	Systems Management: Usage Metering Function (ISO 10164-10), Draft, 1993
ITU-TS X.743	Systems Management, Test Management Function (ISO 10164-12), Draft, 1993
ITU-TS X.744	Systems Management: Software Management Function (ISO 10164-sw), Draft, 1993
ITU-TS X.745	Systems Management: Time Management Function (ISO 10164-tm), Draft, 1993
ITU-TS X.746	Systems Management: Scheduling Function (ISO 10164-15), Draft, 1993
ITU-TS X.747	Systems Management: General Relationship Function (ISO 10164-rm), Draft, 1993
ITU-TS X.748	Systems Management: Response Time Monitoring Function (ISO 10164-rtm), Draft, 1993
ITU-TS X.749	Systems Management: Management Domain Management Function (ISO 10164-md), Draft, 1993
ITU-TS X.750	Systems Management: Management Knowledge Management Function (ISO 10164-16), Draft, 1993
ITU-TS X.751	Systems Management: Change Over Function (ISO 10164-co), Draft, 1993
ITU-TS X.752	Systems Management: Enhanced Event Control Function (ISO 10164-ev), Draft, 1993

F. OSI REGISTRATION AUTHORITIES:

ISO/IEC 9834-1:1993•	Procedures for Specific OSI Registration Authorities, Part 1: General Procedures (X.660)
	PDAM 1 — *Object Identifier Component Attribute Type in Annex B to Accommodate "Short Form Names"*
	WDAM 2 — Incorporate Definition of Root Arcs of Object Identifier Tree
ISO/IEC 9834-2•	Procedures for Specific OSI Registration Authorities, Part 2: Registration Procedures for Document Types
ISO/IEC 9834-3•	Procedures for Specific OSI Registration Authorities, Part 3: Procedures for Specific Registration of Joint Object Identifier Component Values for Joint ISO-ITU-TS Use
	WDAM 1 — Amendment 1: Alignment with ISO/IEC 9834-1:1993
ISO/IEC 9834-4•	Procedures for Specific OSI Registration Authorities, Part 4: Register of VTE Profiles
ISO/IEC 9834-5•	Procedures for Specific OSI Registration Authorities, Part 5: Register of VT Control Objects
ISO/IEC 9834-6•	Procedures for Specific OSI Registration Authorities, Part 6: Registration Authority Procedures for Application Process Titles and Application Entity Titles (X.665)
WD 9834-7	Procedures for Specific OSI Registration Authorities, Part D: Registration of Application Contexts
WD 9834-8	Procedures for Specific OSI Registration Authorities, Part E: Registration of System Titles
WD 9834-11	Procedures for Specific OSI Registration Authorities, Part F: Registration of Authentication Mechanisms
WD 9834-B	Procedures for Specific OSI Registration Authorities, Part B: Registration of Abstract Syntaxes
WD 9834-C	Procedures for Specific OSI Registration Authorities, Part C: Registration of Transfer Syntaxes
ISO/IEC TR 9973	Registration of Graphical Items
SC21 N 5758	Discussion Paper on Conformance and Registration, BSI
SC21 N 6903	Request for the Work on "Procedures for the Operation of Registration Authorities: Application Processes and Application Entities" to Become Collaborative
ITU-TS I.414	Overview of Recommendations on Layer 1 for ISDN and B-ISDN Customer Accesses
ITU-TS X.660	Procedures for the Operation of OSI Registration Authorities: General Procedures (ISO 9834-1), 1992
ITU-TS X.662	Procedures for the Operation of OSI Registration Authorities: Registration of Object Identifier Component Values for Joint ISO-CCITT Use (ISO 9834-3), Draft, 1993

ITU-TS X.665	Procedures for the Operation of OSI Registration Authorities: Application Processes and Applicaion Entitits (ISO 9834-6), 1992

G. OSI CONFORMANCE TESTING:

ISO/IEC 9646-1•	OSI Conformance Testing Methodology and Framework, Part 1: General Concepts	
	AM 1	Protocol Profile and Multi-Protocol Testing
	AM 2	Multi-Party Testing Methodology
	Cor 1	Technical Corrigendum 1
DIS 9646-1.2	OSI Conformance Testing Methodology and Framework, Part 1: General Concepts, Second Edition, (incorporating all approved amendments)	
ISO/IEC 9646-2•	OSI Conformance Testing Methodology and Framework, Part 2: Abstract Test Suite Specification (ITU-TU X.291)	
	Annex	Guidelines for PICS Proformas
	AM 1	Protocol Profile and Multi-Protocol Testing
	AM 2	Multi-Party Testing Methodology
DIS 9646-2.2	OSI Conformance Testing Methodology and Framework, Part 2: Abstract Test Suite Specification, second edition	
ISO/IEC 9646-3•	OSI Conformance Testing Methodology and Framework, Part 3: Executable Test Derivation (X.292)	
	AM 1	TTCN Extensions
	DAM 2	Further TTCN Extensions
ISO/IEC 9646-4•	OSI Conformance Testing Methodology and Framework, Part 4: Test Realization (X.293)	
	AM 1	Protocol Profile and Multi-Protocol Testing
	AM 2	Multi-Party Testing Methodology
DIS 9646-4.2	OSI Conformance Testing Methodology and Framework, Part 4: Test Realization, Edition 2	
ISO/IEC 9646-5•	OSI Conformance Testing Methodology and Framework, Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process (Test Execution) (X.294)	
	AM 1	Protocol Profile and Multi-Protocol Testing
	AM 2	Multi-Party Testing Methodology
	Cor 1	Technical Corrigendum 1
DIS 9646-5.2	OSI Conformance Testing Methodology and Framework, Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process, second edition	
ISO/IEC 9646-6	OSI Conformance Testing Methodology and Framework, Part 6: Protocol Profile Test Specification	
DIS 9646-7	OSI Conformance Testing Methodology and Framework, Part 7: Requirements and Guidelines on Implementation Conformance Statement (ICS) and ICS Proformas	
ISO/IEC 10025-1•	Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network Service (CONS), Part 1: General Principles	
ISO/IEC 10025-2•	Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network data Transfer, Part 1: Abstract Service Definition	
ISO/IEC 10025-3•	Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network Service (CONS), Part 3: Transport Test Management Protocol Specification, 1993	
ISO/IEC 10641	Conformance Testing of Implementations of Graphics Standards, 1993	
ISO/IEC 10729-1	Conformance Test Suite for the Presentation Protocol, Part 1: Test Suite Structure and Test Purposes for the Presentation Protocol, November 1993	
DIS 10729-2	Conformance Test Suite for the Presentation Layer, Part 2: Test Suite for ASN.1 Encodings and Test Purposes for Presentation Protocol, November 1993	
WD 10729-3	Conformance Test Suite for the Presentation Layer, Part 3: Common Presentation Abstract Test Suite, October 1991	
ISO/IEC 10739-1	Conformance Test Suite for 9041 - Virtual Terminal Basic Class Protocol, Part 1: Test Suite Structure and Test Purposes	
SC21 N 6160	Catalogue of PICS Proforma Notations	
SC21 N 6639	Proposed Liaison Statement to SC21/WG4 Regarding General and Dependent Conformance	
SC21 N 6640	Health Warning Regarding General and Dependent Conformance JTC1-ITU-TS Interim Meeting on Conformance	
SC21 N 6810	UK Position on General and Dependent Conformance	
SC21 N 6819	Report of the ISO/IEC-ITU-TS Joint OSI Conformance Group Interim Meeting Held in Durham, North Carolina	
SC21 N 6881	Liaison Statement to SC21/WG1 from SC18 on Conformance in Response to SC18 N 3291	
SC21 N 6891	Liaison Statement to SC18 and SC21 on the Status of CCITT X.400/X.500 PICS Proforma Recommendations and Future Collaborative Work	
SC21 N 7016	Presentation Connection-Oriented Abstract Test Suite (ATS), Specific Partial ATS	
SC21 N 7069	Draft Answer to Q1/49.9 on Long-term Solution to General and Dependent Conformance	

SC21 N 7073	Proposed New Sub-Question Q1/49.9 on Long-term Solution to General and Dependent Conformance
SC21 N 7074	Liaison Statement to JTC1/SGFS on Conformance Testing
SC21 N 7075	Liaison Statement to SC6 on ICS Proforma
SC21 N 7076	Liaison Statement to SC18 on Conformance Testing
SC21 N 7078	Draft Answer to Q1/49.8 - Conformance and Registration
SC21 N 7079	Working Draft Answer to Q1/63.2 - Testability of Managed Objects
SC21 N 7080	Liaison Statements to EWOS on Conformance Testing
SC21 N 7995	Working Draft on Formal Methods in Conformance Testing
SC21 N 8010	Open Systems Assessment Methodology
SC21 N 8011	Conformance Testing of OSI Protocols over OSI Services Provided by Non-OSI Protocols
SC21 N 8016	Extensions to ISO 9646 on Testing of OSI Protocols over OSI Services Provided by Non-OSI Protocols
SC21 N 8264	Liaison Statement to SC21/WG1 Conformance Group on Collaborative Work, ITU-TS/SG7, October 1993
SC21 N 8355	Liaison Statement to SC21/WG1 and SC22/WG15 on Conformance Testing, December 1993
SC21/WG1 N 1140	UK Discussion Paper on Conformance Testing for OSI Security
SC21/WG1 N 1156	Clarification on Use of the PICS
ITU-TS X.290	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: General Concepts (DIS 9646-1), 1992
ITU-TS X.291	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: Abstract Test Suite Specifications (ISO 9646-2), 1992
ITU-TS X.292	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: TTCN (ISO 9646-3), 1992
ITU-TS X.293	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: Test Realization (ISO 9646-4), 1992
ITU-TS X.294	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: Requirements on Test Labsoratories and Clients for Conformance Assessment Process (ISO 9646-5), 1992
ITU-TS X.295	Conformance Testing Methodology and Framework - Protocol Profile Test Specification (ISO 9646-6), Draft, 1993
ITU-TS X.296	Conformance Testing Methodology and Framework - Implementation Conformance Statements (ISO 9646-7), Draft, 1993

H. TAXONOMY AND PROFILES:

STANAG 4406• Military Message Handling System, Draft, NATO UNCLASSIFIED (cf. ISO 10021, 10611)

- Main Body, Draft
- Annex A—MMHS Extensions to ISO 10021 Series, Draft
- Annex B—Security Aspects of MMHS (under development)
- Annex C—Alpha Profile Set (a delta specification to EWOS profiles): AMH1x(M) on Common Facilities and AMH9x(M) on Military Messaging, Draft
- Annex D—Alpha/ACP 127 Gateway (under development)
- Annex E—Alpha/MMHS(84) Gateway (under development)
- Annex F—Alpha/MHS(88) Gateway (under development)
- Annex G—Beta Profile Set (under development)
- Annex H—Beta/ACP 127 Gateway (under development)
- Annex I—Beta/Alpha Gateway (under development)

STANAG 4407• System Management, Draft, NATO UNCLASSIFIED (cf. ISO 10165-1, 10165-2, 10165-4, 10164, 11183, 12059, 12060)

- Main Body, Preliminary Draft
- Annex A—Security of Management (under development)
- Annex B—Military Features, Preliminary Draft
- Annex C—The Development of NSPs for Systems Management, Preliminary Draft
- Annex D—NSP zzzz: Basic Systems Management, Preliminary Draft (STANAG 4407-1)

STANAG 4408• Connection-mode Transport Service over Connectionless-mode Network Service

- Part 1: Subnetwork Type Independent Requirements for Group TA, Preliminary Draft (cf. ISO 10608-1)
- Part 2: TA5n(M) Subnetwork Type Dependent, Media Independent Requirements for LANs, Preliminary Draft (cf. ISO 10608-2)
- Part 3: TA51(M) Subnetwork Type Dependent, Media Independent Requirements for CSMA/CD LANs, Preliminary Draft (cf. ISO 10608-2)
- Part 4: TA54(M) Subnetwork Type Dependent, Media Independent Requirements for FDDI LANs, Preliminary Draft (cf. ISO 10608-6)

STANAG 4409• Connection-mode Transport Service over Connection-mode Network Service (Military)
- Part 1: Definition of Profiles TC1111(M)/TC1121(M), Preliminary Draft (cf. ISO 10609-6)
- Part 2: Subnetwork Type Independent Requirements for Group TC, Preliminary Draft (cf. ISO 10609-2)
- Part 3: TA51(M) Subnetwork Type Dependent Requirements for Permanent Access to a Packet Data Network Using Virtual Call, Preliminary Draft (cf. ISO 10609-9)

STANAG 4410• Connectionless-mode Transport Service over Connectionless-mode Network Service
- Part 1: Subnetwork Type Independent Requirements for Group UA, Preliminary Draft

STANAG 4413• Relaying the Connectionless-mode Network Service
- Part 1: Subnetwork Type Independent Requirements for Group RA (cf. ISO 10613-1) (under development)
- Part 2: Subnetwork Type Dependent, Media Independent Requirements for LANs (cf. ISO 10613-2) (under development)
- Part 3: ISDN Subnetwork Dependent, Media Dependent Requirements for Circuit Switched B-Channel Operation (under development)
- Part 4: Profile RA51.4212 (under development)

ISO/IEC TR 10000-1• International Standardized Profiles (ISPs), Part 1: Taxonomy Framework, Edition 2

WDTR 10000-1.3 Framework of International Standardized Profiles (ISPs), Part 1: Taxonomy Framework, Edition 3

ISO/IEC TR 10000-2• Framework and Taxonomy of International Standardized Profiles, Part 2: Taxonomy of OSI Profile, Edition 2

DTR 10000-2.3• Framework and Taxonomy of International Standardized Profiles, Part 2: Taxonomy of OSI Profile, Edition 3

WDTR 10000-3 Framework and Taxonomy of International Standardized Profiles, Part 3: New Taxonomy Parts

ISO/IEC ISP 10607-1• ISPs AFT nn - File Transfer, Access, and Management, Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM
- DAM 1 Additional Specifications for COBOL Document Types

ISO/IEC ISP 10607-2• ISPs AFT nn - File Transfer, Access, and Management, Part 2: Definition of Document Types, Constraint Sets and Syntaxes
- DAM 1 Additional Definitions
- DAM 2 Additional Specifications for COBOL Document Types
- DAM 3 FTAM Constraint Set and Document Type for CGM

ISO/IEC ISP 10607-3• ISPs AFT nn - File Transfer, Access, and Management, Part 3: AFT 11 - Simple File Transfer Service (Unstructured)

ISO/IEC ISP 10607-4• ISPs AFT nn - File Transfer, Access, and Management, Part 4: AFT 12 - Positional File Transfer Service
- DAM 1 Additional Specifications for COBOL Document Types

ISO/IEC ISP 10607-5• ISPs AFT nn - File Transfer, Access, and Management, Part 5: AFT 22 - Positional File Access Service
- DAM 1 Additional Specifications for COBOL Document Types

ISO/IEC ISP 10607-6• ISPs AFT nn - File Transfer, Access, and Management, Part 6: AFT 12 - File Management Service

ISO/IEC ISP 10607-x ISPs AFT nn - File Transfer, Access and Management, Part x: AFT 13 - Full File Transfer (Hierarchical), Draft, 1993

ISO/IEC ISP 10607-y ISPs AFT nn - File Transfer, Access and Management, Part y: AFT 23 - Full File Access (Hierarchical), Draft, 1993

ISO/IEC ISP 10607-z ISPs AFT nn - File Transfer, Access and Management, Part z: AFT 4 - Filestore Management Profiles, Draft, 1993

ISO/IEC ISP 10608-1• ISPs TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 1: General Overview and Subnetwork-Independent Requirements, 1992

ISO/IEC ISP 10608-2• ISPs TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 2: TA51 Profile Including Subnetwork-dependent Requirements for CSMA/CD Local Area Networks, 1992

DISP 10608-3 ISPs TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 3: TA 52, LAN, Token Bus: CLNS

ISO/IEC 10608-4• ISP TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 4: TA53 COTS over CLNS, LICI, Token Ring LAN

ISO/IEC ISP 10608-5• ISPs TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 5: TA1111/TA1121 Profiles Including Subnetwork-dependent Requirements for X.25 Packet Switched Data Networks Using Switched Virtual Circuits, 1992

DISP 10608-6• ISPs TA nnnn - Connection-mode Transport Service over Connectionless Network Service, Part 6: TA54 Profile

DISP 10608-13 International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless Network Service, Part 13: LAN-Dependent Requirements for Token Ring MAC and PHY

DISP 10608-14•	ISPs TA nnnn - Connection-mode Transport Service over Connectionless Network Service, Part 14: MAC, PHY, PMD Sublayer Dependent State Management Requirement over FDDI LAN Subnetwork
ISO/IEC ISP 10609-1	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 1: Subnetwork-type Independent Requirements for Group TB, 1992
ISO/IEC ISP 10609-2•	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 2: Subnetwork-type Independent Requirements for Group TC, 1992
ISO/IEC ISP 10609-3	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 3: Subnetwork-type Independent Requirements for Group TD, 1992
ISO/IEC ISP 10609-4	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 4: Subnetwork-type Independent Requirements for Group TE, 1992
ISO/IEC ISP 10609-5	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 5: Definition of Profile TB 1111/TB 1121, 1992
ISO/IEC ISP 10609-6•	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 6: Definition of Profile TC 1111/TC 1121, 1992
ISO/IEC ISP 10609-7	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 7: Definition of Profile TD 1111/TD 1121, 1992
ISO/IEC ISP 10609-8	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 8: Definition of Profile TE 1111/TE 1121, 1992
ISO/IEC ISP 10609-9•	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 9: Subnetwork-type Dependent Requirements for Network Layer, Data Link Layer, and Physical Layer Concerning Permanent Access to a Packet Switched Data Network Using Virtual Call, 1992
pDISP 10609-10	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 10, 1993
pDISP 10609-11	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 11, 1993
pDISP 10609-12	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 12: TC51 Profile, 1993
pDISP 10609-13	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 13: TC53 Profile, 1993
pDISP 10609-14	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 14: COTS Classes 0 and 2, CONS, LLC2, Token Ring LAN, 1993
pDISP 10609-20	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 20: TC/TD nnnn, Overview of the Generalized Multipart ISP structure for TC and TD Group Profiles for OSI Usage of ISDN, February 1993 (review ended June 1993)
pDISP 10609-21	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 21: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer and Data Link Layer Concerning End Systems Attached to an ISDN Subnetwork for B-Channel X.25 DTE-to-DTE Operation, February 1993 (review ended June 1993)
pDISP 10609-22	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 22: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer and Data Link Layer Concerning End Systems Attached to an ISDN Subnetwork for B-Channel X.25 DTE-to-DCE Operation, February 1993 (review ended June 1993)
pDISP 10609-23	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 23: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer and Data Link Layer for Data Transfer Concerning Packet-Switched Mode ISDN Virtual Calls: B-Channel Access Case, February 1993 (review ended June 1993)
pDISP 10609-24	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 24: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer Using Q.931 - Circuit-Switched Case, February 1993 (review ended June 1993)
pDISP 10609-25	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 25: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Outgoing Call of a Packet-Switched Mode ISDN in Case B Using Virtual Calls, February 1993 (review ended June 1993)
pDISP 10609-26	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 26: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Outgoing Call of a Packet-Switched Mode ISDN in Case B Using Virtual Calls, February 1993 (review ended June 1993)
pDISP 10609-27	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 27: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Incoming Call of a

	Packet-Switched Mode ISDN in Case B Using Virtual Calls, February 1993 (review ended June 1993)
pDISP 10609-28	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 28: TC/TD nnnn, Subnetwork Type Dependent Requirements for Data Link Layer for End Systems Attached to an ISDN Subnetwork, February 1993 (review ended June 1993)
pDISP 10609-29	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 29: TC 1131, ISDN B-Channel Virtual Call, Permanent Access to a PSDN - Transport Protocol Classes 0 and 2, February 1993 (review ended June 1993)
pDISP 10609-30	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 30: TC 1131, ISDN B-Channel Virtual Call, Switched Access to a PSDN - Transport Protocol Classes 0 and 2, February 1993 (review ended June 1993)
DISP 10609-31♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 31: TC 1231, ISDN B-Channel Virtual Call, Switched Access to a PSDN, 1993
DISP 10609-32♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 32: TC 4111, ISDN B-Channel X.25 DTE to DTE, Semi-permanent Service, 1993
DISP 10609-33♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 33: TC 4112, ISDN B-Channel X.25 DTE, Circuit-mode Service, 1993
DISP 10609-34♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 34: TC 43111, ISDN D-Channel Access Virtual Call, Packet-mode Service, Without Q.931, 1993
DISP 10609-35♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 35: TC 43112, ISDN D-Channel Access Virtual Call, Packet-mode Service, with Q.931, 1993
DISP 10609-36♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 36: TC 43211, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, Without Q.931, 1993
DISP 10609-37♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 37: TC 43212, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, with Q.931, 1993
DISP 10609-38♦	ISPs TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 38: TC 4331, ISDN B-Channel Demand Access Virtual Call, Packet-mode Service, 1993
pDISP 10609-40	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 40: TD 1131, ISDN B-Channel Virtual Call, Permanent Access to a PSDN - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-41	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 41: TD 1231, ISDN B-Channel Virtual Call, Switched Access to a PSDN - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-42	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 42: TD 4111, ISDN B-Channel, X.25 DTE-to-DTE, Semi-Permanent Service - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-43	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 43: TD 4211, ISDN B-Channel, X.25 DTE-to-DTE, Circuit-mode Service - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-44	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 44: TD 43111, ISDN D-Channel Access Virtual Call, Packet-mode Service, Without Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)
pDISP 10609-45	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 45: TD 43112, ISDN D-Channel Access Virtual Call, Packet-mode Service, With Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)
pDISP 10609-46	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 46: TD 43211, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, Without Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)
pDISP 10609-47	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 47: TD 43212, ISDN B-Channel, Permanent Access Virtual Call, Packet-mode Service, With Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)
pDISP 10609-48	International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 48: TD 43212, ISDN B-Channel, Demand Access Virtual Call, Packet-mode Service - Transport Protocol Classes 0, February 1993 (review ended June 1993)
ISO/IEC ISP 10610-1	ISPs FOD nn, Part 1: FOD 11 Profile, Simple Document Structure - Character Content Only, April 1992
DISP 10611-1♦	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 1: Service Support, 1993

DISP 10611-2◆	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 2: Specification of ROSE, RTSE, ACSE, Presentation, and Session for Use by MHS, 1993
DISP 10611-3◆	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 3: AMH11: Message Transfer (P1), 1993
DISP 10611-4◆	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 4: AMH12: MTS Access (P2), 1993
DISP 10611-5◆	ISPs AMH1n - Message Handling Systems - Common Messaging, Parat 5: AMH13: MS Access (P7), 1993
pDISP 10612-1	ISPs RD nn.nn, Part 1: RD 5p.5q Profile, Relaying MAC Using Transparent Bridging - General Overview and Subnetwork Independent Requirement, 1993
pDISP 10612-2	ISPs RD nn.nn, Part 2: RD 5p.5q Profile, Relaying MAC Using Transparent Bridging - CSMA/CD LAN Subnetwork Dependent Media Dependent, 1993
pDISP 10612-3	International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 3: RD 5p.5q Profile, Token Ring LAN Subnetwork-Dependent Media-Dependent Requirements, May 1993 (balloting ended September 1993)
DISP 10612-4◆	ISPs RD nn.nn, Part 4: RD 51.51 Profile, Relaying MAC, 1993
pDISP 10612-5	International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 5: RD 51.54 Profile, CSMA/CD - FDDI, May 1993 (balloting ended September 1993)
pDISP 10612-6	International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 6: RD 51.53 Profile, FDDI - FDDI, May 1993 (balloting ended September 1993)
pDISP 10612-7	ISPs RD nn.nn, Part 7: RD 51.53 Profile, MAC Service Relay Using Transparent Bridging, CSMA/CD - Token Ring, 1993
pDISP 10612-8	ISPs RD nn.nn, Part 8: RD 53.53 Profile, MAC Service Relay Using Transparent Bridging, Token Ring - Token Ring, 1993
pDISP 10612-9	ISPs RD nn.nn, Part 9: RD 53.54 Profile, MAC Service Relay Using Transparent Bridging, Token Ring - FDDI, 1993
pDISP 10613-1◆	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 1: Relay Function, 1993
pDISP 10613-2◆	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 2: LAN Subnetwork, 1993
DISP 10613-3◆	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 3: CSMA/CD LAN Subnetwork, 1993
DISP 10613-4	International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 4: FDDI LAN Subnetwork-Dependent Media-Dependent Requirements, 1993 (review ended April 1993)
pDISP 10613-5◆	ISPs RA nn.nn -Relaying the Connectionless-mode Network Service, Part 5: RA51.51 Profile, Relaying CLNS - CSMA/CD, 1993
pDISP 10613-6	International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 6: RA 51.54, CSMA/CD LAN and FDDI LAN, 1993 (review ended April 1993)
pDISP 10613-7◆	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 7: PSDN Subnetwork Media Dependent VC Permanent Access, 1993
pDISP 10613-8◆	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 8: RA51.1111 Profile, 1993
pDISP 10613-9◆	ISPs RA nn.nn - Relaying the Connectionless-mode Network Service, Part 9: RA51.1121 Profile, 1993
pDISP 10614-1	ISPs RC nn.nn - Relaying X.25 PLP, Part 1: General Overview and Subnetwork Independent Requirement, 1993
pDISP 10614-2	ISPs RC nn.nn - Relaying X.25 PLP, Part 2: LAN Subnetwork Dependent Media Independent Requirement, 1993
pDISP 10614-3	ISPs RC nn.nn - Relaying X.25 PLP, Part 3: CSMA/CD LAN Subnetwork Dependent Media Dependent, 1993
pDISP 10614-4	ISPs RC nn.nn - Relaying X.25 PLP, Part 4: PSDN Subnetwork Type Dependent Requirement, 1993
DISP 10614-5◆	ISPs RC nn.nn - RC51.1111, Relaying X.25, Part 5, 1993
DISP 10614-6◆	ISPs RC nn.nn - RC51.1121, Relaying X.25, Part 6, 1993
DISP 10615-1◆	ISPs ADI nn -- OSI Directory, Part 1: ADI 11, DUA support of Directory access, January 1993
DISP 10615-2◆	ISPs ADI nn -- OSI Directory, Part 2: ADI 12, DSA support of Directory access, January 1993
DISP 10615-3◆	ISPs ADI nn -- OSI Directory, Part 3: ADI 21, DSA responder role, July 1993
DISP 10615-4◆	ISPs ADI nn -- OSI Directory, Part 4: ADI 22, DSA initiator role, July 1993
pDISP 10615-5	ISPs ADI nn -- OSI Directory, Part 5: ADI 31, DUA Support of Distributed Operations, 1993
pDISP 10615-6	ISPs ADI nn -- OSI Directory, Part 6: ADI 32, DSA Support of Distributed Operations, 1993
pDISP 10615-7	ISPs ADI nn -- OSI Directory, Part 7: ADI 41, Strong Authentication, 1993
pDISP 10616	ISP FDI 11 - Directory Data Definitions - Common Directory Use, September 1993
ISO/IEC ISP 11181-1	ISP FOD26 - Enhanced Document Structure - Character, Raster Graphics and Geometric Graphics Content Architecture, April 1992

ISO/IEC ISP 11182-1	ISP FOD36 - Extended Document Structure - Character, Raster Graphics and Geometric Graphics Content Architecture, April 1992
ISO/IEC ISP 11183-1♦	ISPs AOM 1n - OSI Management - Management Communications Protocols, Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by ROSE and CMISE, Revised Edition, December 1992
ISO/IEC ISP 11183-2♦	ISPs AOM 1n - OSI Management - Management Communications Protocols, Part 2: CMISE/ROSE for AOM 12, Enhanced Management Communications, 1993
pDISP 11183-x	ISPs AOM 1n - OSI Management - Management Communications Protocols, Part x: Development of PTS for CMIP (AOM 11, AOM 12), 1993
pDISP 11184-1	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 1: FVT 121 - S-mode Forms VTE Profile, 1993
pDISP 11184-2	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 2: FVT 122 - S-mode Paged VTE Profile, 1993
pDISP 11184-3	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 3: FVT 111 - A-mode Telnet Profile
pDISP 11184-4	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 4: FVT 112 - A-mode Scroll VTE Profile
pDISP 11184-5	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 5: FVT 113 - A-mode CCITT X.3 PAD Interworking
pDISP 11184-6	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 6: FVT 114 - A-mode Transparent VTE Profile
pDISP 11184-7	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 7: FVT 115 - A-mode Generalized Telnet VTE Profile, 1993
pDISP 11185-1	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 1: FVT 211, FVT 212, Sequenced and Unsequenced Application Control Objects, 1993
pDISP 11185-2	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 2: FVT 213, FVT 214, Sequenced and Unsequenced Terminal Control Objects, 1993
pDISP 11185-3	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 3: FVT 215, FVT 216, Application RIO Record Locating Control Object and Terminal RIO Record Notification Control Object, 1993
pDISP 11185-4	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 4: FVT 217, Horizontal Tabulation Control Object, 1993
pDISP 11185-5	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 5: FVT 218, Logical Image Control Object, 1993
pDISP 11185-6	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 6: FVT 219, Status Message Control Object, 1993
pDISP 11185-7	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 7: FVT 220, Entry-control Control Object, 1993
pDISP 11185-8	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 8: FVT 221, Forms Field Entry Instruction Control Object (FEICO) No. 1, 1993
pDISP 11185-9	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 9: FVT 222, Paged Field Entry Instruction Control Object (PEICO) No. 1, 1993
pDISP 11185-10	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 10: FVT 231, Forms Field Entry Pilot Control Object (FEPCO) No. 1, 1993
pDISP 11185-11	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 11: FVT 232, Paged Field Entry Pilot Control Object (PEPCO) No. 1, 1993
pDISP 11185-12	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 12: FVT 251, Terminal Conditions Control Object No. 1
pDISP 11185-13	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 13: FVT 2111, Waiting Time Control Object (pDISP expected 1995)
pDISP 11185-14	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 14: FVT 2112, Printer Control Object, 1993
pDISP 11185-15	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 15: FVT 2113, Field Definition Control Object, 1993
pDISP 11185-16	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 16: FVT 2114, Terminal Signal Titles Control Object, 1993
pDISP 11185-17	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 17: FVT 2115, Form Help Text Control Object, 1993
pDISP 11186-1	ISPs FVT 3nn - Virtual Terminal Basic Class - Register of Assignment Type Definitions, Part 1: FVT 321, Font Assignment Type No. 1
DISP 11187-1♦	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 1: AVT 22, S-mode Forms Application Profile, 1993
DISP 11187-2♦	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 2: AVT 23, S-mode Paged Application Profile, 1993
pDISP 11187-3	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 3: S-mode ISPICS Requirements List No. 1

pDISP 11187-4	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 4, S-mode ISPICS Requirements (IPRL) List No. 1, Supporting Layers List No. 1
pDISP 11187-6	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 6: AVT 13, A-mode Scroll Application Profile
pDISP 11187-7	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 7: AVT 14, A-mode CCITT X.3 PAD Application Profile
pDISP 11187-8	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 8: AVT 15, A-mode Transparent Application Profile
pDISP 11187-9	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 9: AVT 16, A-mode Generalized Telnet Application Profile, 1993
pDISP 11187-10	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 10: AVT 17, A-mode ISPICS Requirements List No. 1
pDISP 11188-1	ISPs - Common Upper Layer Requirements, Part 1: Basic Connection Oriented Requirements, 1993
pDISP 11188-2	ISPs - Common Upper Layer Requirements, Part 2: ROSE Based Requirements, 1993
pDISP 11188-3	ISPs - Common Upper Layer Requirements, Part 3: Minimal OSI Upper Layer Facilities, July 1993
DISP 11189	ISP FDI2 - MHS Use of Directory, 1993
DISP 11190	ISP FDI3 - FTAM Use of Directory, 1993
DISP 12059-0	ISPs - Management Functions - Common Information for Management Functions, Part 0: Common Definitions for Management Function Profiles, 1992
DISP 12059-1•	ISPs - Management Functions - Common Information for Management Functions, Part 1: Object Management, 1992
DISP 12059-2•	ISPs - Management Functions - Common Information for Management Functions, Part 2: State Management, 1992)
DISP 12059-3•	ISPs - Management Functions - Common Information for Management Functions, Part 3: Attributes for Representing Relationships, 1992
DISP 12059-4•	ISPs - Management Functions - Common Information for Management Functions, Part 4: Alarm Reporting, 1992
DISP 12059-5•	ISPs - Management Functions - Common Information for Management Functions, Part 5: Event Report Management, 1992
DISP 12059-6•	ISPs - Management Functions - Common Information for Management Functions, Part 6: Log Control, 1992
DISP 12060-1•	ISPs AOMnnn - OSI Management - Management Functions, Part 1: AOM 211, General Management Capability, 1992
DISP 12060-2	ISPs AOMnnn - OSI Management - Management Functions, Part 2: AOM 212, Alarm Reporting and State Management Capabilities, 1992
DISP 12060-3	ISPs AOMnnn - OSI Management - Management Functions, Part 3: AOM 213, Alarm Reporting Capabilities, 1992
DISP 12060-4•	ISPs AOMnnn - OSI Management - Management Functions, Part 4: AOM 221, General Event Report Management, 1992
DISP 12060-5•	ISPs AOMnnn - OSI Management - Management Functions, Part 5: AOM 231, General Log Control, 1992
DISP 12060-w	ISPs AOMnnn - OSI Management - Management Functions, Part w: AOM 242, Security Protocols (ISP expected November 1993)
DISP 12060-x	ISPs AOMnnn - OSI Management - Management Functions, Part x: AOM 251, General Performance Profile (ISP expected September 1994)
DISP 12060-y	ISPs AOMnnn - OSI Management - Management Functions, Part y: AOM 252x, Metric Objects
DISP 12060-z	ISPs AOMnnn - OSI Management - Management Functions, Part z AOM 253x, Summarization Objects
DISP 12061-1	ISPs ATP nn - OSI Distributed Transaction Processing, Part 1: Introduction, 1993
DISP 12061-2	ISPs ATP nn - OSI Distributed Transaction Processing, Part 2: Support of the OSI TP APDUs, 1993
DISP 12061-3	ISPs ATP nn - OSI Distributed Transaction Processing, Part 3: Support of the CCR Protocols, 1993
DISP 12061-4	ISPs ATP nn - OSI Distributed Transaction Processing, Part 4: Support of ACSE, Presentation and Session Protocols, 1993
DISP 12061-5	ISPs ATP nn - OSI Distributed Transaction Processing, Part 5: ATP 11, Application Supported Transactions with Polarized Control, 1993
DISP 12061-6	ISPs ATP nn - OSI Distributed Transaction Processing, Part 6: ATP 12, Application Supported Transactions with Shared Control, 1993
DISP 12061-7	ISPs ATP nn - OSI Distributed Transaction Processing, Part 7: ATP 21, Provider Supported Transactions in Unchained Mode with Polarized Control, 1993
DISP 12061-8	ISPs ATP nn - OSI Distributed Transaction Processing, Part 8: ATP 22, Provider Supported Transactions in Unchained Mode with Shared Control, 1993
pDISP 12061-9	ISPs ATP nn - OSI Distributed Transaction Processing, Part 9: ATP 31, Provider Supported Transactions in Chained Mode with Polarized Control, 1993
pDISP 12061-10	ISPs ATP nn - OSI Distributed Transaction Processing, Part 10: ATP 32, Provider Supported Transactions in Chained Mode with Shared Control, 1993

pDISP 12061-11	ISPs ATP nn - OSI Distributed Transaction Processing, Part 11: TP Transaction Recovery Application Context, 1993
pDISP 12061-x	ISPs ATP nn - OSI Distributed Transaction Processing, Part x: Systems Profiling for TP, 1993
pDISP 12061-y	ISPs ATP nn - OSI Distributed Transaction Processing, Part y: Development of PTS for TP, 1993
pDISP 12062-1	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 1: IPM MHS Service Support, August 1993 (review ended December 1993)
pDISP 12062-2	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 2: AMH 21, IPM Content, August 1993 (review ended December 1993)
pDISP 12062-3	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 3: AMH 22, IPM Requirements for Message Transfer (P1), August 1993 (review ended December 1993)
pDISP 12062-4	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 4: AMH 23, IPM Requirements for MTS Access (P3), August 1993 (review ended December 1993)
pDISP 12062-5	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 5: IPM Requirements for Enhanced MS Access (P7), August 1993 (review ended December 1993)
pDISP 12063	International Standardized Profiles AMH 3 - Message Handling Systems, 1993
pDISP 12064-1	International Standardized Profiles FOD nnn - ODA - Open Document Format: Image Applications - Simple Document Structure - Raster Graphics Content Architecture, Part 1: FOD 112, Document Applications Profile, August 1993 (balloting ended December 1993)
pDISP 12065-1	International Standardized Profiles ALD 1n - Library and Documentation - Search and Retrieve, Part 1: Specification of ACSE, Presentation, and Session Protocols for Use by Library and Documentation, August 1993
pDISP 12066-1	International Standardized Profiles ALD 2n - Library and Documentation - Interlibrary Loan, Part 1: Generic, August 1993
pDISP 12066-2	International Standardized Profiles ALD 2n - Library and Documentation - Interlibrary Loan, Part 2: Using Connection-Oriented ACSE, August 1993
SC21 N 6776	Framework & Taxonomy of International Standardized Profiles - Directory of ISPs & Profiles Contained Therein
SC21 N 7197	Response to the Request from SGFS for Comments on Issues Regarding Registration and ISPs
SC21 N 7360	Development of the SGFS Procedures to Cover Other TCs and the Open System Environment (SGFS N 590)
SC21 N 8118	Report from the SC21 ISP Meeting, 23 June 1993, Yokohama, June 1993
SGFS N 1056	EWOS Major Comments on the Third Working Draft of TR 10000 Part 3 (ISO/IEC JTC1/SGFS N 1024) and Proposals for Change, EWOS, November 1993

I. MODELLING FACILITIES:

JTC1 N 2621	Proposal for an NWI: Conceptual Schema Modelling Facility, August 1993 [SC21 N 8060, June 1993] (balloting ended in November 1993) (WD expected July 1995, CD July 1996, DIS July 1997, and IS July 1998)
JTC1 N 2775	Summary of Voting on Document JTC1 N 2621, Proposal for a New Work Item: Conceptual Schema Modelling Facility, December 1993
JTC1 N 2835	Report from ISO/IEC JTC1/SC21 Chairman on Activities Related to Application Program Interfaces (APIs) and Modelling Facilities (MFs), January 1994
SC21 N 8056	SC21 SWG-MF Meeting, June 1993, Yokohama, July 1993
SC21 N 8057	Recommendation to Progress Work on the Use of Standard Data Modelling Facilities in the Preparation of International Standards, SWG-MF, July 1993
SC21 N 8058	Final Recommendations of the SC21 Special Working Group on Modelling Facilities (SWG-MF), SWG-MF, July 1993
SC21 N 8059	Response to the SC21 Chairman from the SC21 Special Working Group on Modelling Facilities (SWG-MF), SWG-MF, July 1993
SC21 N 8061	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to ISO/IEC JTC1/SC18 Liaison Statement, SWG-MF, July 1993
SC21 N 8062	SC21 Special Working Group on Modelling Facilities (SWG-MF) Liaison Statement to ISO/IEC JTC1/SC14, SWG-MF, July 1993
SC21 N 8063	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to ISO/IEC JTC1/WG3 Open edi Liaison Report, SWG-MF, July 1993
SC21 N 8064	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to ISO/TC46/SC4 Liaison Statement, SWG-MF, July 1993
SC21 N 8065	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to JTC1/SC21/WG7 Liaison Statement, SWG-MF, July 1993
SC21 N 8127	Liaison Information on Modelling Facility Interim Work, SC21 SWG-MF, June 1993
SC21 N 8282	Calling Notice and Draft Agenda for the Interim Meeting of the SC21/WG3 Rapporteur Group on Conceptual Schema Modelling Facilities, Aix en Provence, 17-21 January 1994, October 1993

SC21 N 8305	A Data Modelling Facility: JDMF/MODEL-1992, Japan, October 1993
SC21/WG3 N 1644	Technical Report on the Semantic Unification of Meta-Model, Volume 1, Semantic Unification of Static Models, US National Body, Nnovember 1993
SC21/WG3 N 1645	Knowledge Interchange Format (KIF), US National Body, Nnovember 1993
SC21 WG3 N 1646	Proposed Working Draft for Base Document for Conceptual Schema Modelling Facilities

J. OPEN SYSTEM ENVIRONMENT (OSE) AND PROGRAMMING INTERFACES

JTC1 N 2835	Report from ISO/IEC JTC1/SC21 Chairman on Activities Related to Application Program Interfaces (APIs) and Modelling Facilities (MFs), January 1994
JTC1 N 2836	JTC1/SC21 Reports on Application Program Interfaces (APIs), January 1994
SGFS N 983	UK Discussion Paper Relating to User Requirements Relevant to Open Systems Assessment Methodology, July 1993
SGFS N 1078	Draft Guide to the POSIX Open System Environment (P1003.0/D16.1), IEEE Computer Society, December 1993
SGFS N 1003	Modification of SD-1, SGFS Procedures, for Adoption of PTSs and APIs, August 1993
SGFS N 1043	Liaison Statement to SGFS and EWOS/EG-OSE, OIW, November 1993
SGFS N 1065	US Comments on OIW Liaison Statement to SGFS and EWOS/EG-OSE, August 1993
SGFS N 1087	Liaison Statement to SC21/SWG-PS, SGFS, December 1993
SGFS N 1089	White Paper on OSE Profiling Concepts, SGFS, December 1993 (materiel offered for integration in ISO/IEC TR 10000)
SGFS N 1090	Liaison Statement to JTC1 on the Subject of PAS and APIs, December 1993
SGFS N 1099	Draft Minutes of the SGFS Authorized Subgroup Meeting in Amsterdam, 29 November to 3 December 1993, SGFS, December 1993
SGFS N 1098	Resolutions Adopted by the SGFS Authorized Subgroup Meeting in Amsterdam, 29 November to 3 December 1993, SGFS, December 1993
SC21 N 8010	Proposal for an NP on Open Systems Assessment Methodology, July 1993
SC21 N 8013	Liaison Statement to JTC1/SWG-CA, JTC1/SGFS, EWOS, OIW, and AOW on Open Systems Assessment Methodology, August 1993
SC21 N 8109	Proposed New Question Q3/011, "Harmonization of Client/Server Capabilities," SC21/WG3, September 1993
SC21 N 8258	Corrected Liaison Statement to SC21 Entitled, "Comments on the First Draft Report on the New Work Area on Programmatic Interfaces," SC18, October 1993
SC21 N 8316	Comments on Standardized Programmatic Interfaces, USA, October 1993
SC21 N 8320	UK Position on Programmatic Interface Standardization, UK, November 1993
SC21 N 8397	Outline Contribution to Future Work as Proposed in SC21 N 8045 Rev 2, SC21 SWG-SPI Meeting 8-11 November 1993 in Torina, January 1994

II. LAYER 1: PHYSICAL LAYER[19]

A. General
B. Mechanical
C. Functional
D. Procedural
E. Local Area Networks

A. GENERAL:

STANAG 4251♦	NATO Reference Model for OSI - Layer 1 (Physical Layer) Service Definition, Draft
STANAG 4261♦	NATO Reference Model for OSI - Layer 1 (Physical Layer) Protocol Specification, Draft
ISO 6951	Information Processing - Processor System Bus Interface (Eurobus A)
ISO 9160	Physical Layer Interoperability Requirements
ISO 9316	Small Computer System Interface (SCSI)
DIS 9318-1	Intelligent Peripheral Interface, Part 1: Physical Level
ISO 9318-2	Intelligent Peripheral Interface, Part 2: Device Specific Command Set for Magnetic Disk Drives
ISO 9318-3	Intelligent Peripheral Interface, Part 3: Device Generic Command Set for Magnetic and Optical Disk Drives
ISO 9318-4	Intelligent Peripheral Interface, Part 4: Device Generic Command Set for Magnetic Tape Drives
DIS 9324	Storage Module Interfaces
ISO/IEC 10022♦	Physical Service Definition (X.211)
DIS 10222	Enhanced Small Device Interface
ITU-TS V.7♦	Definition of Terms Concerning Data Communication over Telephone Network
ITU-TS X.211	Physical Service Definition of OSI for CCITT Applications (ISO 10022)
ITU-TS X.281	Elements of Management Information Related to the OSI Physical Layer (ISO 13642), Draft, 1993

B. MECHANICAL:

ISO 2110♦	25-Pin DTE/DCE Interface Connector and Pin Assignments
	AM 1 — Interface Connector and Contact Number Assignments for a DTE/DCE for Data Signalling Rates Above 20 kbit/s
ISO 2593:1984♦	34-Pin DTE/DCE Interface Connector and Pin Assignments
ISO 4902♦	37-Pin DTE/DCE Interface Connector and Pin Assignments
ISO 4903♦	15-Pin DTE/DCE Interface Connector and Pin Assignments
ISO/TR 7477♦	Arrangements for DTE/DTE Physical Connection Using V.24 and X.24 Interchange Circuits
ISO 8481♦	DTE/DTE Physical Connection Using X.24 Interchange Circuits with DTE-Provided Timing
ISO/IEC 8877♦	Interface Connector and Contact Assignments for ISDN Basic Access Interface Located at Reference Points S and T
	AM 1 — Standard ISDN Basic Access TE Connecting Cord
ISO/IEC 10173♦	ISDN Primary Access Connector at Reference Points S and T
ISO/IEC 11569	26-Pole Interface Connector Mateability Dimensions and Contact Number Assignments, 1993
CD 11573	Synchronization Methods and Technical Requirements for Private Integrated Services Networks
CD 11574	Private Integrated Services Network - Circuit Mode 64 kbit/s Bearer Services - Service Definition - Functional Capabilities and Information Flows
ITU-TS I.340	ISDN Connection Types

C. ELECTRICAL:

ISO 8482♦	Twisted Pair Multipoint Interconnections
ISO 9549♦	Galvanic Isolation of Balanced Interchange Circuits, October 1990
ITU-TS Q.700♦	Signaling System No. 7 (SS7) Overview
ITU-TS Q.701-Q.710♦	Signaling System No. 7 (SS7) Message Transfer Part
ITU-TS Q.711-Q.716♦	Signaling System No. 7 (SS7) Signalling Connection Control Part (SCCP)
ITU-TS Q.720-Q.729♦	Signaling System No. 7 (SS7) Telephone User Part (TUP)

---

19 The symbol ♦ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

ITU-TS Q.730-Q.739◆	Signaling System No. 7 (SS7) ISDN Supplementary Services
ITU-TS Q.760-Q.769◆	Signaling System No. 7 (SS7) Description of the ISDN User Part (ISUP)
ITU-TS Q.770-Q.779◆	Signaling System No. 7 (SS7) Transaction Capabilities (TC)
ITU-TS V.5	Data Signalling Rates for Synchronous Data Transmission in the General Switched Telephone Network
ITU-TS V.6	Data Signalling Rates for Synchronous Data Transmission on Leased Telephone-Type Circuits
ITU-TS V.13	Simulated Carrier Control
ITU-TS V.14	Transmission of Start-Stop Characters over Synchronous Bearer Channels
ITU-TS V.17	A 2-wire Modem for Facsimile Applications with Data Signaling Rates of up to 9,600 bit/s for Use on the General Switched Telephone Network and on Leased Telephone-Type Circuits
ITU-TS V.32 bis	A Duplex Model Operating at Data Signalling Rates of up to 14,400 bit/s for Use on the General Switched Telephone Network and on Leased Point-to-Point 2-wire Telephone-Type Circuits
ITU-TS V.38	A 48/56/64 kbit/s Data Circuit Terminating Equipment Standardized for Use on Digital Point-to-Point Leased Circuits
ITU-TS V.42 Rev 1	Error-Correcting Procedures for DCEs Using Asynchronous-to-Synchronous Conversion
ITU-TS V.42 bis	Data Compression Procedures for Data Circuit Terminating Equipment (DCE) Using Error Correcting Procedures

D. FUNCTIONAL:

ISO/IEC 7480◆	Start-Stop Transmission Signal Quality at DTE/DCE Interfaces, Second Edition
ISO 9543◆	Synchronous Transmission Signal Quality at DTE/DCE Interfaces
ITU-TS I.411 Rev 1	ISDN User-Network Interfaces—Reference Configuration
ITU-TS I.412	ISDN User-Network Interfaces—Interface Structures and Access Capabilities
ITU-TS X.1 Rev 1◆	International User Classes of Service in Public Data Networks and Integrated Services Digital Networks (ISDNs)
ITU-TS X.2 Rev 1	International Data Transmission Services and Optional User Facilities in Public Data Networks and ISDNs
ITU-TS X.3 Rev 1	Packet Assembly/Disassembly Facility (PAD) in a Public Data Network (PDN)
ITU-TS X.4	General Structure of Signals of International Alphabet No. 5 Code for Data Transmission over Public Data Networks
ITU-TS X.5	Facsimile Packet Assembly/Disassembly Facility (FPAD) in a Public Data Network
ITU-TS X.6	Multicast Service Definition
ITU-TS X.7	Technical Characteristics of Data Transmission Services
ITU-TS X.10◆	Categories of Access for DTE to Public Data Transmission Services Provided by PDNs and/or ISDNs through Terminal Adaptors
ITU-TS X.24◆	List of Definitions for Interchange Circuits Between DTE and DCE on Public Data Networks
ITU-TS X.26/V.10◆	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communications
ITU-TS X.27/V.11◆	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communications
ITU-TS X.28 Rev 1	DTE/DCE Interface for a Start/Stop Mode DTE Accessing the PAD in a PDN Situated in the Same Country
ITU-TS X.29 Rev 1	Procedures for the Exchange of Control Information and User Data Between a PAD Facility and a Packet Mode DTE or Another PAD
ITU-TS X.30/I.461	Support of X.21, X.21 bis, and X.20 bis Based Data Terminal Equipment's (DTEs) by an Integrated Services Digital Network (ISDN)
ITU-TS X.31/I.462 Rev 1◆	Support of Packet Mode Terminal Equipment by an ISDN
ITU-TS X.38	G3 Facsimile Equipment/DCE Interface for G3 Facsimile Equipment Accessing the Facsimile Packet Assembly/Disassembly Facility (FPAD) in a Public Data Network Situated in the Same Country
ITU-TS X.39	Procedures for the Exchange of Control Information and User Data Between a Facsimile Packet Assembly/Disassembly (FPAD) Facility and a Packet Mode DTE or Another FPAD
ITU-TS X.50	Fundamental Parameters of a Multiplexing Scheme for the International Interface Between Synchronous Data Networks
ITU-TS X.50bis	Fundamental Parameters of a 48-kbit/s User Data Signalling Rate Transmission Scheme for the International Interface Between Synchronous Data Networks
ITU-TS X.51	Fundamental Parameters of a Multiplexing Scheme for the International Interface Between Synchronous Data Networks Using 10-bit Envelope Structure
ITU-TS X.51bis	Fundamental Parameters of a 48-kbit/s User Data Signalling Rate Transmission Scheme for the International Interface Between Synchronous Data Using 10-bit Envelope Structure Networks
ITU-TS X.52	Method of Encoding Anisochronous Signals into a Synchronous Use Bearer
ITU-TS X.53 Rev 1	Numbering of Channels on International Multiplex links at 64 kbit/s
ITU-TS X.54	Allocation of Channels on International Multiplex Links at 64 kbit/s
ITU-TS X.55	Interface Between Synchronous Data Networks Using a 6 + 2 Envelope Structure and Single Channel Per Carrier (SCPC) Satellite Channels

ITU-TS X.56	Interface Between Synchronous Data Networks Using an 8+2 Envelope Structure and Single Channel Per Carrier (SCPC) Satellite Channels
ITU-TS X.57	Method of Transmitting a Single Lower Speed Data Channel on a 64 kbit/s Data Stream
ITU-TS X.58	Fundamental Parameters of a Multiplexing Scheme for the International Interface Between Synchronous Non-Switched Data Networks Using No Envelope Structure
ITU-TS X.60	Common Channel Signalling for Circuit Switched Data Applications
ITU-TS X.61/Q.741	Signalling System No. 7 - Data User Part
ITU-TS X.70	Terminal and Transit Control Signalling System for Start-Stop Services on International Circuits Between Anisochronous Data Networks
ITU-TS X.71	Decentralized Terminal and Transit Control Signalling System on International Circuits Between Synchronous Data Networks
ITU-TS X.75 Rev 1♦	Packet-Switched Signalling System Between Public Networks Providing Data Transmission Services, 1993
ITU-TS X.7x	Signalling System Between Public Networks Providing Frame Relaying Data Transmissional Services, Draft, 1993 (approval date November 1994)
ITU-TS X.80	Interworking of Interexchange Signalling Systems for Circuit Switched Data Services
ITU-TS X.81	Interworking Between an ISDN Circuit Switched and a Circuit Switched Public Data Network (CSPDN)
ITU-TS X.82	Detailed Arrangements for Interworking Between CSPDNs and PSPDNs Based on Recommendation T.70
ITU-TS X.92	Hypothetical Reference Connections for Public Synchronous Data Networks
ITU-TS X.96 Rev 1	Call Progress Signals in Public Data Networks
ITU-TS X.121	International Numbering Plan for Public Data Networks
ITU-TS X.122/E.166	Numbering Plan Interworking for the W.164 and X.121 Numbering Plans
ITU-TS X.130	Call Processing Delays in Public Data Networks when Providing International Synchronous Circuit-Switched Data Services
ITU-TS X.131	Call Blocking in Public Data Networks when Providing International Synchronous Circuit-Switched Data Services
ITU-TS X.134	Portion Boundaries and Packet Layer Reference Events: Basis for Defining Packet-Switched Performance Parameters
ITU-TS X.135	Speed of Service (Delay or Throughput) Performance Values for Public Data Networks when Providing International Packet-Switched Services
ITU-TS X.136	Accuracy and Dependability Performance Values for Public Data Networks when Providing International Packet-Switched Services
ITU-TS X.137	Availability Performance Values for Public Data Networks when Providing International Packet-Switched Services
ITU-TS X.138.	Measurement of Performance Values for Public Data Networks when Providing International Packet-Switched Services
ITU-TS X.139	Echo, Drop, Generator and Test DTE's for Measurement of Performance Values for Public Data Networks when Providing International Packet-Switched Services
ITU-TS X.140	General Quality of Service Parameter for Communication Via Public Data Networks
ITU-TS X.180	Administrative Arrangements for International Closed User Groups (CUGs)
ITU-TS X.181	Administrative Arrangements for the Provision of International Permanent Virtual Circuits (PVCs)
ITU-TS X.3x	Access to Packet Switched Data Transmission Services Provided by PSPDN or ISDN via Frame Relaying PDNs or ISDN Providing Frame Mode Bearer Service, Draft, 1993 (approval target November 1994)
ITU-TS X.asp	Multi-Aspect PAD Protocol Definitions-1, Draft, 1993 (approval target November 1994)
ITU-TS X.asp+	Multi-Aspect PAD Protocol Definitions-2, Draft, 1993 (approval target 1996)
ITU-TS X.atc	Address Translation Capability in Public Data Networks, Draft, 1993 (approval target November 1994)
ITU-TS X.fiq	User Information Transfer Parameters and Specifications for Data Networks Providing International Frame Relay PVC Service, Draft, 1993 (approval date November 1994)
ITU-TS X.fru	Interface Between DTE and DCE for Public Data Network Prroving Frame Relay Data Transmission Service, Draft, 1993 (approval target November 1994)
ITU-TS X.isp	Inter-Service Protocol for a Multicast Service, Draft, 1993 (approval target June 1995)
ITU-TS X.map	Multi-Aspect PAD Framework, Draft, 1993 (approval target February 1994)
ITU-TS X.mcp	Procedures for the Provision of a Basic Multicast Service for DCEs Operating Using Recommendation ITU-TS X.25, Draft, 1993 (approval target November 1994)
ITU-TS X.mcp+	Procedures for the Provision of an Enhanced Multicast Service for DCEs Operating Using Recommendation ITU-TS X.25 and Requiring Additional Protocol, Draft, 1993 (approval target 1996)
ITU-TS X.mpc	Encapsulation in ITU-TS X.25 Packets of Various Protocols Including Frame Relay, Draft, 1993 (approval target November 1994)

E. PROCEDURAL:

ISO 8480	DTE/DCE Back-Up Control Operation Using the 25-Pole Connector
ISO 9067	Automatic Fault Isolation Procedures Using Test Loops
ITU-TS I.420	Basic User-Network Interface (ISDN)
ITU-TS I.421	Primary Rate User-Network Interface (ISDN)
ITU-TS I.430 Rev 1	Basic User-Network Interface—Layer 1 Specification (ISDN)
ITU-TS I.431 Rev 1•	Primary Rate User-Network Interface—Layer 1 Specification (ISDN)
ITU-TS I.432 Rev 1•	B-ISDN Network Interface—Physical Layer Specification
ITU-TS I.460•	Multiplexing, Rate Adaptation and Support of Existing Interfaces (ISDN)
ITU-TS I.461•	Support of X.21, X.21 bis, and X.20 bis Based DTEs by an ISDN (X.30)
ITU-TS I.462•	Support of Packet Mode Terminal Equipment by an ISDN (X.31)
ITU-TS I.463•	Support of DTEs with V-Series Type Interfaces by an ISDN
ITU-TS I.464•	Multiplexing, Rate Adaptation, and Support of Existing Interfaces for Restricted 64 kbit/s Transfer Capability
ITU-TS I.465	Support by an ISDN of DTEs with V-Series Type Interfaces with Provisions for Statistical Multiplexing
ITU-TS I.470	Relationship of Terminal Functions to ISDN
ITU-TS V.10/X.26•	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communication
ITU-TS V.11/X.27•	Electrical Characteristics for Balanced Double-Current Interchange Circuits for General Use With Integrated Circuit Equipment in the Field of Data Communications
ITU-TS V.20	Telex and Gentex Signalling on Radio Channels (Synchronous 7-Unit Systems Affording Error Correction by Automatic Repetition)
ITU-TS V.24•	List of Definitions for Interchange Circuits Between DTE and DCE
ITU-TS V.25	Automatic Answering Equipment and/or Parallel Automatic Calling Equipment on the General Switched Telephone Network Including Procedures for Disabling of Echo Control Devices for Both Manually and Automatically Established Calls
ITU-TS V.28 Rev 1•	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits
ITU-TS V.31	Electrical Characteristics for Single-Current Interchange Circuits Controlled by Contact Closure
ITU-TS V.31 bis	Electrical Characteristics for Single-Current Interchange Circuits Using Opto Couplers
ITU-TS V.35•	Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits
ITU-TS V.36•	Modems for Synchronous Data Transmission Using 60-108 kHz Group Band Circuits
ITU-TS V.37•	Synchronous Data Transmission at a Data Signalling Rate Higher than 72 kbit/s Using 60-108 kHz Group Band Circuits
ITU-TS V.54	Loop Test Devices for Modems
ITU-TS X.20 Rev 1	Interface Between DTE and DCE for Start-Stop Transmission Services on Public Data Networks
ITU-TS X.20 bis	Use on Public Data Networks of DTE Which Is Designed for Interfacing to Asynchronous Duplex V-Series Modems
ITU-TS X.21•	Interface Between DTE and DCE for Synchronous Operation on Public Data Networks
ITU-TS X.21 bis•	Use on Public Data Networks of DTE Which Is Designed for Interfacing to Synchronous V-Series Modems
ITU-TS X.22	Multiplex DTE/DCE Interface for User Classes 3-6
ITU-TS X.31 Rev 1•	Support of Packet Mode Terminal Equipment by an ISDN
ITU-TS X.32 Rev 1•	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Accessing a Packet Switched PDN Through a Public Switched Telephone Network or a Circuit Switched PDN
ITU-TS X.150	Principles of Maintenance Testing for Public Data Networks Using DTR and DCE Test Loops, 1988
ITU-TS X.160	Architecture for Customer Network Management Services for Public Data Networks, Draft, 1993
ITU-TS X.161	Definition of Customer Network Management Services for Public Data Networks, Draft, 1993
ITU-TS X.162	Definition of Management Informaton for the Customer Network Management Services for Public Data Networks, Draft, 1993

F. LOCAL AREA NETWORKS (LANs):

IEC 847	Characteristics of LANs, 1988		
IEC/TR 907	Local Area Networks CSMA/CD 10 Mbit/s Baseband Planning and Installation Guide		
ISO 8802-1•	LANs, Part 1: General Introduction		
DIS 8802-1.2	LANs, Part 1: General Introduction with System Load Protocol		
ISO 8802-2•	LANs, Part 2: Logical Link Control		
DIS 8802-2.2	LANs, Part 2: Logical Link Control, Edition 2		
		Cor 1	Technical Corrigendum 1
		DAM 1	Flow Control Techniques for Bridged LANs
		DAM 2	Type 3 Operation - Acknowledge Connectionless Service
		DAM 3•	PICS Proforma
		DAM 4	Editorial Changes and Technical Corrections

	PDAM 5	Bridged LAN Source Routing Operations by End Systems	
ISO/IEC 8802-3◆	LANs, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) - Access Method and Physical Layer Specifications		
	DAM 6	Summary of IEEE 802.3 First Maintenance Ballot	
	DAM 7	LAN Layer Management	
	DAM 9	Twisted Pair, Medium Attachment Unit, and Baseband Medium Specifications, Type 10BASET	
	PDAM 11	Hub Management, March 1992	
	PDAM 13	Attachment Unit Interface Cable Conformance Test, March 1992	
	PDAM 15	Corrections and Updates 2 & 3, March 1992	
	PDAM 17	PICS Proforma for 10 BASE-T, March 1992	
ISO/IEC 8802-4◆	LANs, Part 4: Token-Passing Bus Access Method and Physical Layer Specifications		
ISO/IEC 8802-5◆	LANs, Part 5: Token Ring Access Method and Physical Layer Specifications		
DIS 8802-6◆	LANs, Part 6: Distributed Queue Dual Bus (DQDB) Media Access Control (MAC)		
ISO/IEC 8802-7	LANs, Part 7: Slotted Ring Access Method and Physical Layer Specification		
DIS 8802-9◆	LANs, Part 9: Integrated Voice and Data (IVD) LAN		
CD 8802-51	LANs, Part 51: MAC Sublayer Conformance Test Purposes		
ISO/IEC 8881◆	Use of the X.25 Packet Level Protocol (PLP) in Local Area Networks		
ISO 9314-1◆	Fiber Distributed Data Interface (FDDI), Part 1: Token Ring Physical Layer Protocol (PHY)		
ISO 9314-2◆	FDDI, Part 2: Token Ring Media Access Control (MAC)		
ISO/IEC 9314-3◆	FDDI, Part 3: Physical Layer Medium Dependent (PMD)		
ISO/IEC 9314-4◆	FDDI-Part 4: Single-Mode Fiber/Physical Layer Medium Dependent		
DIS 9314-5◆	FDDI-Part 5: Hybrid Ring Control (FDDI-II)		
CD 9314-6	FDDI-Part 6: Station Management (SMT) Standard		
ISO/IEC TR 9578	Communication Interface Connectors Used in LANs		
DIS 10038◆	MAC Sublayer Interconnection (MAC Bridging)		
	PDAM 1	Specification of Management Information for CMIP	
	DAM 2	Source Routing Supplement	
ISO/IEC 10039◆	MAC Service Definition		
ISO/IEC TR 10178	Structure and Coding of Link Service Access Point Addresses in LANs		
ISO/IEC TR 10738	Token Ring Access Method and Physical Layer Specifications - Recommended Practice for Use of Unshielded Twisted Pair Cable (UTP) for Token Ring Data Transmission at 4 Mbit/s, 1993		

(This page intentionally left blank)

III. LAYER 2: DATA LINK LAYER[20]

A. General
B. Character-Oriented Service (Basic Mode)
C. Bit-Oriented Service (HDLC Procedures)
D. Integrated Services Digital Network (ISDN)
E. Error Correction and Conformance Test Suite

A. GENERAL:

STANAG 4252◆	NATO Reference Model for OSI - Layer 2 (Data Link Layer) Service Definition	
STANAG 4262◆	NATO Reference Model for OSI - Layer 2 (Data Link Layer) Protocol Specification	
ISO 8886◆	Data Link Service Definition for OSI	
ISO/IEC TR 10171◆	List of Standard Data Link Layer Protocols that Utilize HDLC Classes of Procedures	
	PDAM 1	Registration of XID Format Identifiers and Private Parameter Set Identifiers
DIS 10742	Specification of the Elements of Management Information Related to OSI Data Link Layer Standards, 1993	
SC21 N 6346	Liaison Statement to JTC1/SC21 on Data Link Layer Security	
ITU-TS X.212	Data Link Service Definition of OSI for CCITT Applications (ISO 8886), 1988	
ITU-TS X.282	Elements of Management Information Related to the OSI Data Link Layer (ISO 10742), Draft, 1993	

B. CHARACTER-ORIENTED SERVICE (BASIC MODE):

ISO 1155	Use of Longitudinal Parity to Detect Errors in Information Messages
ISO 1177	Character Structure for Start/Stop and Synchronous Character Oriented Transmission
ISO 1745	Basic Mode Control Procedures for Data Communication Systems
ISO 2111	Basic Mode Control Procedures - Code Independent Information Transfer
ISO 2628	Basic Mode Control Procedures - Complements
ISO 2629	Basic Mode Control Procedures - Conversational Information Message Transfer

C. BIT-ORIENTED SERVICE (HIGH-LEVEL DATA LINK CONTROL PROCEDURES [HDLC]):

ISO 3309:1984◆	HDLC - Frame Structure, Edition 3	
ISO 3309:1991	HDLC - Frame Structure, Edition 4	
	AM 2	Extended Transparency Options for Start/Stop Transmission
	PDAM 3	Seven-bit Transparency Options for Start/Stop Transmission
ISO 4335:1984◆	HDLC - Elements of Procedures, Edition 3	
ISO 4335:1991	HDLC - Elements of Procedures, Edition 4	
	AM 4	Flow Control Unnumbered Information (FUI)
	PDAD 5	Multi-Selective Reject
ISO 7478◆	Multilink Procedures	
	Cor 1	Technical Corrigendum 1
ISO 7776◆	HDLC - Description of the X.25 LAPB-Compatible DTE Data Link Procedures	
	Cor 1-3	Technical Corrigenda 1-3
	AM 1	Conformance Requirements
ISO 7809:1984◆	HDLC - Consolidation of Classes of Procedures, Edition 1	
ISO 7809:1991	HDLC - Consolidation of Classes of Procedures, Edition 2	
	AM 5	Connectionless Class of Procedure
	AM 6	Extended Transparency Option
	AM 7	Multi-Selective Reject
	PDAM 9	Seven-bit Transparency Option for Start/Stop Transmission
ISO 8471◆	HDLC Balanced Classes of Procedures - Data Link Layer Address Resolution/ Negotiation in Switched Environments	

---

20 The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

ISO 8885:1987•	HDLC - General Purpose XID Frame Information Field Content and Format, Edition 1	
ISO 8885:1991	HDLC - General Purpose XID Frame Information Field Content and Format, Edition 2	
	AM 3	Definition of a Private Parameter Negotiation Data Link Layer Subfield
	AM 4	Extended Transparency Option
	AM 5	Multi-Selective Reject
	PDAM 6	Seven-bit Transparency Option for Start/Stop Transmission
	PDAM 7	Frame Check Sequence Negotiation Using the Parameter Negotiation Subfield
DIS 9234	Industrial Asynchronous Data Link for Two-Way Simultaneous or Two-Way Alternate Mode	
ITU-TS T.71•	LAPB Extended for Half-Duplex Physical Level Facility	

D. INTEGRATED SERVICES DIGITAL NETWORK (ISDN):

ITU-TS I.440•	ISDN User-Network Interface Data Link Layer—General Aspects
ITU-TS I.441•	ISDN User-Network Interface Data Link Layer—Specification

E. ERROR CORRECTION AND CONFORMANCE TEST SUITE:

ISO/IEC 8882-2	X.25-DTE Conformance Testing, Part 2: Data Link Conformance Test Suite
DTR 10174	Logical Link Control (Type 2 Operation) Test Purposes
ITU-TS X.141	General Principles for the Detection and Correction of Errors in Public Data Networks

IV. LAYER 3: NETWORK LAYER[21]

A. General
B. Packet-Switched Service
C. Connectionless Service
D. Integrated Services Digital Network (ISDN)
E. Routing and Relay
F. Networking and Interworking
G. Automatic Calling/Answering Equipment
H. Circuit Switched Service
I. Local Area Networks (LANs)

A. GENERAL:

STANAG 4253◆	NATO Reference Model for OSI - Layer 3 (Network Layer) Service Definition
STANAG 4263◆	NATO Reference Model for OSI - Layer 3 (Network Layer) Protocol Specification
ISO 8348◆	Network Service Definition, Edition 2
ISO 8648	Internal Organization of the Network Layer, February 1988
ISO/IEC 8880-1◆	Protocol Combination to Provide and Support the OSI Network Service, Part 1: General Principles
ISO/IEC 8880-2◆	Protocol Combination to Provide and Support the OSI Network Service, Part 2: Provision and Support of the Connection-Mode Network Service
	DAM 1 — Addition of the ISDN Environment
	PDAM 2 — Addition of the PSTN and CSDN Environments
ISO/IEC 8880-3◆	Protocol Combination to Provide and Support the OSI Network Service, Part 3: Provision and Support of the Connectionless-Mode Network Service
ISO/IEC 8880-4◆	Protocol Combination to Provide and Support the OSI Network Service, Part 4: Interconnection of OSI Environments
ISO/IEC TR 9577◆	Protocol Identification in the OSI Network Layer
ISO/IEC TR 10172◆	Network/Transport Protocol Interworking Specification
ISO/IEC 10177◆	Intermediate-System Support of the OSI Connection-Mode Network Service Using ISO 8208 in Accordance with ISO 10028
ISO/IEC 10733◆	Specification of the Elements of Management Information Related to OSI Network Layer Standards [SC21 N 5560, SC6 6413]
WD 10778	High-Speed Integrated Services Networks and User/Network Interface to High-Speed Integrated Services Networks
DIS 11577◆	Network Layer Security Protocol
ITU-TS T.70◆	Network-Independent Basic Transport Service for the Telematic Services
ITU-TS X.213	Network Service Definition for OSI for CCITT Applications (ISO 8348), 1992
ITU-TS X.263	Network Protocol Identification Mechanism (TR 9577), Draft, 1993
ITU-TS X.273	Network Layer Security Protocol (ISO 11577), Draft, 1993
ITU-TS X.283	Elements of Management Information Related to the OSI Network Layer (ISO 10733), Draft, 1993

B. PACKET-SWITCHED SERVICE:

ISO 8208◆	X.25 Packet Level Protocol (PLP) for DTE
	AM 1 — Alternative Logical Channel Number Allocation
	PDAD 2 — Extensions for Private Switched Use
	AM 3 — Static Conformance Requirements
ISO 8878◆	Use of X.25 to Provide the OSI Connection-Mode Network Service
ISO 8878-2	Use of X.25 to Provide the OSI Connection-Mode Network Service, Part 2: Protocol Implementation Conformance Statement (PICS)
ISO/IEC 8881◆	Use of the X.25 Packet Level Protocol (PLP) in Local Area Networks
ISO 8882◆	X.25-DTE Conformance Testing, Part 1: General Principles
ISO/IEC 8882-1	X.25-DTE Conformance Testing, Part 1: General Principles, Edition 2 of ISO 8882
ISO/IEC 8882-2	X.25-DTE Conformance Testing, Part 2: Data Link Conformance Test Suite

21 The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

ISO/IEC 8882-3	X.25-DTE Conformance Testing, Part 3: Packet Level Conformance Test Suite
ISO/IEC 10588	Use of the X.25 PLP in Conjunction with X.21/X.21 bis to Provide OSI CONS
ISO/IEC 10732	Use of the X.25 PLP to Provide OSI CONS over Telephone Network
ITU-TS X.25 Rev 1◆	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit, 1988 (Revised Edition, 1993)
ITU-TS X.75 Rev 1◆	Packet-Switched Signalling System Between Public Networks Providing Data Transmission Services 1988 (Revised Edition, 1993)
ITU-TS X.223	Use of X.25 to Provide the OSI Connection-Mode Network Service for CCITT Applications (ISO 8878), 1988
ITU-TS X.244	Procedure for the Exchange of Protocol Identification During Virtual Call Establishment on Packet Switched Public Data Networks, 1988
ITU-TS X.612	Provision of the OSI Connection-Mode Network Service by Packet Mode Terminal Equipment Connected to an ISDN, 1992

C. CONNECTIONLESS SERVICE:

ISO 8473◆	Protocol for Providing the Connectionless-Mode Network Service (X.233)	
	PDAD 1	Provision of the Underlying Service Assumed by ISO 8473 over Point-to-Point Subnetworks Which Provide the OSI Data Link Service
	PDAD 2	Estelle Formal Description of ISO 8473
	AD 3	Provision of the Underlying Service Assumed by ISO 8473 over Subnetworks Which Provide the OSI Data Link Service
	PDAM 4	PICS Proforma
	DAM 5◆	Provision of the Underlying Service Assumed by ISO 8473 over ISDN Circuit-Switched B-channels
	Cor 1	Technical Corrigendum 1
DIS 9068◆	Provision of the Connectionless Network Service Using ISO 8208	
DIS 10747◆	Protocol for Exchange of Inter-Domain Routing Information Among Intermediate Systems to Support Forwarding of ISO/IEC 8473 PDUs, 1993	
ITU-TS X.233	Protocol for Providing Connectionless-Mode Network Service (ISO 8473-1), Draft, 1993	

D. ISDN:

ISO/IEC 9574◆	Provision of the OSI Connection-Mode Network Service (CONS) by Packet Mode Terminal Equipment Connected to an Integrated Services Digital Network (ISDN)	
	DAM 1	Provision of the CONS on an ISDN Circuit-Switch Channel Connecting Directly to the Remote Terminal
CD 11571	Addressing in Private Integrated Services Digital Network	
CD 11572	Addressing in Private Integrated Services Network - Circuit Mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol,	
CD 11573	Synchronization Methods and Technical Requirements for Private Integrated Services Networks	
CD 11574	Private Integrated Services Network - Circuit Mode 64 kbit/s Bearer Services - Service Definition - Functional Capabilities and Information Flows	
ITU-TS I.130	Attributes for the Characterization of Telecommunications Services Supported by an ISDN and Network Capabilities of an ISDN	
ITU-TS I.140 Rev 1	Attribute Techniques for the Characterization of Telecommunication Services Supported by an ISDN and Network Capabilities of an ISDN	
ITU-TS I.141	ISDN Network Charging Capabilities Attributes	
ITU-TS I.310 Rev 1	ISDN - Network Functional Principles	
ITU-TS I.311 Rev 1	B-ISDN General Network Aspects	
ITU-TS I.324	ISDN Network Architecture	
ITU-TS I.326	Reference Configurations for Relative Network Resource Requirements	
ITU-TS I.330	ISDN Numbering and Addressing Principles	
ITU-TS I.331	Numbering Plan for the ISDN Era	
ITU-TS I.332	Numbering Principles for Interworking Between ISDNs and Dedicated Networks with Different Numbering Plans	
ITU-TS I.334	Principles Relating ISDN Numbers/Subaddresses to the OSI Reference Model Network Layer Addresses	
ITU-TS I.335	ISDN Routing Principles	
ITU-TS I.350 Rev 1	General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDNs	
ITU-TS I.351 Rev 1	Recommendations in Other Services Including Network Performance Objectives that Apply at Reference Point T of an ISDN	
ITU-TS I.352	Network Performance Objectives for Connection Processing Delays in an ISDN	
ITU-TS I.353	Reference Events for Defining ISDN Performance Parameters	

ITU-TS I.354	Network Performance Objectives for Packet-Mode Communication in an ISDN
ITU-TS I.355	ISDN 64 kbit/s Connection Type Availability Performance
ITU-TS I.361 Rev 1	B-ISDN ATM Layer Specification
ITU-TS I.362 Rev 1	B-ISDN ATM Adaptation Layer (AAL) Functional Description
ITU-TS I.363 Rev 1	B-ISDN ATM Adaptation Layer (AAL) Specification
ITU-TS I.364	Support of Broad Band Connectionless Data Service on B-ISDN
ITU-TS I.370	Congestion Management for the ISDN Frame Relaying Bearer Service
ITU-TS I.371	Traffic Control and Congestion Control in B-ISDN
ITU-TS I.372	Frame Relaying Bearer Service Network-to-Network Interface Requirements
ITU-TS I.373	Network Capabilities to Support Universal Personal Requirements
ITU-TS I.374	Framework Recommendation on Network Capabilities to Support Multimedia Services
ITU-TS I.450◆	ISDN User-Network Interface—Layer 3 General Aspects
ITU-TS I.451◆	ISDN User-Network Interface—Layer 3 Specification for Basic Call Control
ITU-TS I.452	ISDN User-Network Interface—Layer 3 Specification Generic Procedures for the Control of the ISDN Supplementary Services
ITU-TS I.453(?)◆	ISDN User-Network Interface—Protocol for Management General Aspects (Q.940)
ITU-TS I.500 Rev 1	General Structure of the ISDN Interworking Recommendations
ITU-TS I.501	Frame Mode Bearer Services (FMBS) Interworking
ITU-TS I.510 Rev 1	Definitions and General Principles for ISDN Interworking
ITU-TS I.511	ISDN to ISDN Layer 1 Internetwork Interface
ITU-TS I.515 Rev 1	Parameter Exchange for ISDN Interworking
ITU-TS I.520 Rev 1	General Arrangement for Network Interworking Between ISDNs
ITU-TS I.525	Interworking Between ISDN and Networks Which Operate at Bit Rates Less Than 64 kbit/s
ITU-TS I.530 Rev 1	Network Interworking Between an ISDN and a Public Switched Telephone Network (PSTN)
ITU-TS I.540	General Arrangement for Network Interworking Between Circuit Switched Public Data Networks (CSPDNs) and ISDNs for the Provision of Data Transmission Services
ITU-TS I.550	General Arrangement for Network Interworking Between Packet Switched Public Data Networks (PSPDNs) and ISDNs for the Provision of Data Transmission Services
ITU-TS I.570	Public/Private ISDN Interworking
ITU-TS I.580	General Arrangements for Interworking Between B-ISDN and 64 kbit/s Based ISDN

Note: Additional ISDN standards are listed in Section IX.A at the end of this appendix.

E. ROUTING AND RELAY:

ISO 9542◆	End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-Mode Network Service
	Cor 1 — Technical Corrigendum 1
	PDAM 1 — Dynamic Discovery of OSI Addresses by End Systems
ISO/IEC TR 9575◆	OSI Routing Framework
ISO/IEC 10028-1◆	Definition of the Relaying Functions of a Network Layer Intermediate System, Part 1: Connection-mode Network Service, 1993
	PDAM 1 — Connectionless-mode Relaying Functions
ISO/IEC 10028-2◆	Definition of the Relaying Functions of a Network Layer Intermediate System, Part 2: Connectionless Network Service, 1993
ISO/IEC TR 10029◆	Operation of an X.25 Interworking Unit
ISO/IEC 10030	End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP) [SC6 N 5006]
	Cor 1 — Technical Corrigendum 1
	PDAM 1 — Dynamic Discovery of OSI NSAP Addresses by End Systems
	AM 2 — PICS Proforma
	PDAM 3 — Specification of IS-SNARE Interactions
DIS 10030-2	End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8878 (X.25 PLP), Part 2: PICS Proforma
ISO/IEC 10589	Intermediate System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO 8473
DIS 10747◆	Protocol for Exchange of Inter-Domain Routing Information Among Intermediate Systems to Support Forwarding of ISO 8473 PDUs
CD 11571	Addressing in Private Integrated Services Digital Network
CD 11572	Addressing in Private Integrated Services Network - Circuit Mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol
ITU-TS X.110	International Routing Principles and Routing Plan for Public Data Networks, 1988
ITU-TS X.353	Routing Principles for Interconnecting the Maritime Satellite Data Transmission System With Public Data Networks, 1988

F. NETWORKING AND INTERWORKING:

ITU-TS X.300	General Principles and Arrangements for Interworking Between Public Data Networks, and Between PDNs and Other Public Networks
ITU-TS X.301 Rev 1	Description of the General Arrangement for Call Control Within a Subnetwork and Between Subnetworks for the Provision of Data Transmission
ITU-TS X.302	Description of the General Arrangement for Internal Network Utilities Within a Subnetwork and Immediate Utilities Between Subnetworks for the Provision of Data Transmission Services
ITU-TS X.305	Functionalities of Subnetworks Relating to the Support of the OSI Connection-Mode Network Service
ITU-TS X.310	Procedures and Arrangements for DTE Accessing Circuit Switched Digital Data Services Through Analogue Telephone Networks
ITU-TS X.320	General Arrangements for Interworking Between ISDNs for the Provision of Data Transmission Services
ITU-TS X.321/I.540	General Arrangements for Interworking Between Circuit Switched Public Data Networks (CSPDNs) and ISDNs for the Provision of Data Transmission Services
ITU-TS X.322	General Arrangements for Interworking Between Packet Switched Public Data Networks (PSPDNs) and CSPDNs for the Provision of Data Transmission Services
ITU-TS X.323	General Arrangements for Interworking Between PSPDNs
ITU-TS X.324	General Arrangements for Interworking Between PSPDNs and Public Mobile Systems for the Provision of Data Transmission Services
ITU-TS X.325	General Arrangements for Interworking Between PSPDNs and ISDNs for the Provision of Data Transmission Services
ITU-TS X.326	General Arrangements for Interworking Between PSPDNs and Common Channel Signalling Network (CCSN)
ITU-TS X.327	General Arrangements for Interworking Between PSPDNs and Private Data Networks for the Provision of Data Transmission Services
ITU-TS X.340 Rev 1	General Arrangements for Interworking Between PSPDNs and the International Telex Network
ITU-TS X.350	General Interworking Requirements to be Met for Data Transmission in International Public Mobile Satellite Systems
ITU-TS X.351	Special Requirements to be Met for Packet Assembly/Disassembly Facilities (PADs) Located at or in Association with Coast Earth Stations in the Public Mobile Satellite Service
ITU-TS X.352	Interworking Between Packet Switched Public Data Networks and Public Maritime Mobile Satellite Data Transmission Systems
ITU-TS X.353	Routing Principles for Interconnecting Public Maritime Mobile Satellite Data Transmission Systems with Public Data Networks, 1988
ITU-TS X.370	Arrangements for the Transfer of Internetwork Management Information, 1988
ITU-TS X.3fi	General Arrangements for Interworking Between Frame Relaying Public Data Networks and ISDNs, Draft, 1993
ITU-TS X.610	Provision and Support of the OSI Connection-Mode Network Service, 1992
ITU-TS X.612	Provision of the OSI Connection-Mode Network Service by Packet Mode Terminal Equipment Connected to an ISDN, 1992
ITU-TS X.613	Use of ITU-TS X.25 Packet Layer Protocol in Conjunction with ITU-TS X.21/ITU-TS X.21 bis to Provide the OSI Connection-Mode Network Service, 1992
ITU-TS X.614	Use of ITU-TS X.25 Packet Layer Protocol in Conjunction with ITU-TS X.21/ITU-TS X.21 bis to Provide the OSI Connection-Mode Network Service over the Telephone Network, 1992
ITU-TS X.615	Provision of the OSI Connection-Mode Network Service over Frame Relay, 1992
ITU-TS X.620	Provision and Support of the OSI Connection-Mode Network Service over Frame Relay, 1992
ITU-TS X.622	Use of ITU-TS X.25 Packet Layer Protocol in Conjunction with ITU-TS X.21/ITU-TS X.21 bis to Provide the OSI Connection-Mode Network Service over the Telephone Network, 1992
ITU-TS X.623	Use of ITU-TS X.25 Packet Layer Protocol in Conjunction with ITU-TS X.21/ITU-TS X.21 bis to Provide the OSI Connection-Mode Network Service over the Telephone Network, 1992

G. AUTOMATIC CALLING/ANSWERING, EQUIPMENT:

ITU-TS V.25	Automatic Answering Equipment and/or Parallel Automatic Calling Equipment on the General Switched Telephone Network Including Procedures for Disabling of Echo Control Devices for Both Manually and Automatically Established Calls
ITU-TS V.25 bis	Automatic Calling and/or Answering Equipment on the General Switched Telephone Network (GSTN) Using the 100-Series Interchange Circuits

H. CIRCUIT SWITCHED SERVICE:

Covered by CCITT	X.21, X.24, X.26, X.27, ISO 4903, listed under Physical Layer Standards

I. LOCAL AREA NETWORKS (LANs):

DIS 10038•	MAC Sublayer Interconnection (MAC Bridging)
ISO/IEC 10039•	MAC Service Definition

Other standards are covered in the discussion of LAN standards for Layer 1 (Section II)

(This page intentionally left blank)

V. LAYER 4: TRANSPORT LAYER[22]

A. General
B. Connection-Oriented Service
C. Connectionless Service
D. Conformance Testing

A. GENERAL:

STANAG 4254◆	NATO Reference Model for OSI - Layer 4 (Transport Layer) Service Definition		
STANAG 4264◆	NATO Reference Model for OSI - Layer 4 (Transport Layer) Protocol Specification		
ISO 8072◆	Transport Service Definition		
		Cor 1	Technical Corrigendum 1
		AD 1◆	Connectionless-Mode Transmission
ISO/IEC TR 10023◆	A Formal Description of ISO 8072 in LOTOS (awaiting decision concerning further progression)		
ISO/IEC TR 10172◆	Network/Transport Protocol Interworking Specification		
PDTR 10734	Guidelines for Bridged LAN Source Routing Operation by End Systems		
ISO/IEC TR 10735	Standard Group MAC Addresses		
DIS 10736	Transport Layer Security Protocol		
		PDAM 1	Security Association Establishment Protocol
ISO/IEC 10737◆	Specification of Elements of Management Information Related to OSI Transport Layer Standards		
ISO/IEC 10740-1	Text and Office Systems - Referenced Data Transfer, Part 1: Abstract Service Definition		
ISO/IEC 10740-2	Text and Office Systems - Referenced Data Transfer, Part 2: Protocol Specification		
ISO/IEC 11570◆	Transport Protocol Identification Mechanism		
ITU-TS T.70◆	Network-Independent Basic Transport Service for the Telematic Services		
ITU-TS X.214	Transport Service Definition of OSI for CCITT Applications (ISO 8072, 1986)		
ITU-TS X.234	Protocol for Providing the OSI Connectionless-Mode Transport Service, Draft, 1993		
ITU-TS X.264	Transport Protocol Identification Mechanism (ISO 11570), Draft, 1993		
ITU-TS X.274	Transport Layer Security Protocol (ISO 10736), Draft, 1993		
ITU-TS X.284	Elements of Management Information Related to the OSI Transport Layer (ISO 10737), Draft, 1993		

B. CONNECTION-ORIENTED SERVICE:

ISO/IEC 8073◆	Connection Oriented Transport Protocol Specification, Edition 3
ISO/IEC TR 10024◆	A Formal Description of ISO 8073 in LOTOS
pDISP 11188-1	Common Upper Layer Requirements, Part 1: Basic Connection Oriented Requirements
pDISP 11188-2	Common Upper Layer Requirements, Part 2: ROSE Based Requirements
pDISP 11188-3	Common Upper Layer Requirements, Part 3: Minimal OSI Upper Layer Facilities
ITU-TS X.224	Protocol for Providing the OSI Connection-mode Transport Service (ISO 8073), 1988

C. CONNECTIONLESS SERVICE:

ISO 8602◆	Protocol for Providing the Connectionless-Mode Transport Service		
		DAM 1	PICS Proforma

D. CONFORMANCE TESTING:

ISO/IEC 10025-1◆	Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network Service (CONS), Part 1: General Principles
ISO/IEC 10025-2◆	Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network data Transfer, Part 1: Abstract Service Definition
ISO/IEC 10025-3◆	Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network Service (CONS), Part 3: Abstract Test Suite Specification
ISO/IEC 10739-1	Conformance Test Suite for 9041 - Virtual Terminal Basic Class Protocol, Part 1: Test Suite Structure and Test Purposes

---

22 The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

(This page intentionally left blank)

VI. LAYER 5: SESSION LAYER[23]

A. General
B. Connection-Oriented Service
C. Connectionless Service
D. Telematic Services

A. GENERAL:

STANAG 4255◆		NATO Reference Model for OSI - Layer 5 (Session Layer) Service Definition, Draft
STANAG 4265◆		NATO Reference Model for OSI - Layer 5 (Session Layer) Protocol Specification, Draft
ISO 8326◆		Connection Oriented Session Service Definition (X.215)
	AM 4	Additional Synchronization Functionality
	WDAM 5	Removal of Session Layer Serial Number Limitation
DIS 8326.2		Connection Oriented Session Service Definition, Edition 2 (X.215)
	AM 3	Incorporate Additional Synchronization Functionality
	WDAM 4	Removal of Session Layer Serial Number Limitation,
ISO 8327◆		Basic Connection Oriented Session Protocol Specification, Revised Edition, 1990
DIS 8327-1		Basic Connection Oriented Session Protocol, Part 1: Protocol Specification, Edition 2 of ISO 8327 (X.225)
ISO 8327-2◆		Basic Connection Oriented Session Protocol, Part 2: PICS Proforma (X.245)
ISO/IEC TR 9571◆		LOTOS Description of the Session Service (TR has been cancelled now that the Second Edition of Session Service is published)
ISO/IEC TR 9572◆		LOTOS Description of the Session Protocol (TR has been cancelled now that the Second Edition of Session Service is published)
DIS 10168-1◆		Conformance Test Suite for the Session Protocol, Part 1: Test Suite Structure and Test Purposes
CD 10168-2◆		Conformance Test Suite for the Session Protocol, Part 2: Common Session Abstract Test Suite
CD 10168-3◆		Conformance Test Suite for the Session Protocol, Part 3: Abstract Test Suite for the CS Method
DIS 10168-4◆		Conformance Test Suite for the Session Protocol, Part 4: Session Test Management Protocol Specification
SC21 N 6110		Session Layer Extension to Support Re-Use of Transport Connections
ITU-TS X.215		Session Service Definition for OSI for CCITT Applications (ISO 8826), 1988
ITU-TS X.225		Session Protocol Specification for OSI for CCITT Applications (ISO 8327), 1988
ITU-TS X.245		Connectionless-Mode Session Protocol: Protocol Specification (ISO 9548), Draft, 1993

B. CONNECTION-ORIENTED SERVICE:

ISO 8327◆		Basic Connection-Oriented Session Protocol Specification (X.225)
	AM 3	Incorporate Additional Synchronization Functionality
	WDAM 4	Removal of Session Layer Serial Number Limitation,
DIS 8327-1		Basic Connection Oriented Session Protocol, Part 1: Protocol Specification, Edition 2 of ISO 8327 (X.225)
ISO 8327-2◆		Basic Connection Oriented Session Protocol, Part 2: PICS Proforma (X.245)
ITU-TS X.225		Session Protocol Specification for OSI for CCITT Application (ISO 8327), 1988

C. CONNECTIONLESS SERVICE:

ISO 9548◆	Session Connectionless Protocol to Provide Connectionless-Mode Session Service (X.235)
ISO/IEC 9548-2	Session Connectionless Protocol to Provide Connectionless-Mode Session Service, Part 2: PICS Proforma, 1993 (X.255)
ITU-TS X.235	Connectionless-Mode Session Protocol: Protocol Specification (ISO 9548), Draft, 1993
ITU-TS X.255	Connectionless-Mode Session Protocol: PICS Proforma (ISO 9548-2), Draft, 1993

D. TELEMATIC SERVICES:

ITU-TS T.5	General Aspects of Group 4 Facsimile Apparatus

23 The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

ITU-TS T.62 Rev 1	Control Procedures for Teletex and Group 4 Facsimile Services
ITU-TS X.3 Rev 1	Packet Assembly/Disassembly Facility (PAD) in a Public Data Network (PDN)
ITU-TS X.20 Rev 1	Interface Between DTE and DCE for Start-Stop Transmission Services on Public Data Networks
ITU-TS X.28 Rev 1	DTE/DCE Interface for a Start/Stop Mode DTE Accessing the PAD in a PDN Situated in the Same Country
ITU-TS X.29 Rev 1	Procedures for the Exchange of Control Information and User Data Between a PAD and a Packet Mode DTE or Another PAD

VII. LAYER 6: PRESENTATION LAYER[24]

A. GENERAL:

STANAG 4256◆		Presentation Layer Service Definition
STANAG 4266◆		Presentation Layer Protocol Specification
ISO 8822◆		Connection-Oriented Presentation Service Definition (X.216)
	AM 1◆	Connectionless-Mode Presentation Service
	AM 2	Unlimited User Data
	DAM 3	Abstract Syntax Registration
	AM 4	Support of Session Symmetric Synchronization Service
	AM 5	Delivery of Additional Session Synchronization Functionality to the Presentation Service User
DIS 8822.2		Basic Presentation Service Definition, Edition 2
ISO 8823◆		Connection-Oriented Presentation Protocol Specification (X.226)
	AM 2	Unlimited User Data
	DAM 3	Transfer Syntax Registration
	AM 4	Support of Session Symmetric Synchronization Service
	AM 5	Additional Synchronization Functionality to the Presentation Service User
DIS 8823-1		Connection Oriented Presentation Protocol, Part 1: Protocol Specification, Edition 2 of ISO 8823
ISO/IEC 8823-2		Connection-Oriented Presentation Protocol Specification, Part 2: Presentation Protocol Implementation Conformance Statement (PICS) Proforma (X.246)
ISO/IEC 10729-1		Conformance Test Suite for the Presentation Protocol, Part 1: Test Suite Structure and Test Purposes
DIS 10729-2		Conformance Test Suite for the Presentation Protocol, Part 2: Test Suite for ASN.1 Encodings and Test Purposes for Presentation Protocol
WD 10729-3		Conformance Test Suite for the Presentation Layer, Part 3: Common Presentation Abstract Test Suite
SC21 N 6985		Request for Comments on Compression in Presentation Layer
SC21 N 7032		Liaison Statement to SC18 Concerning the Use of Distinguished Encoding Rules in Document SC21 N 6876
ITU-TS X.216		Presentation Service Definition for OSI for CCITT Applications (ISO 8822), 1988
ITU-TS X.226		Presentation Protocol Specification for OSI for CCITT Application (ISO 8823), 1988
ITU-TS X.246		Connection-Mode Presentation Protocol: PICS Proforma (ISO 8823-2), Draft, 1993

B. CONNECTIONLESS SERVICE:

ISO 8822 AM 1◆	Connection-Oriented Presentation Service Definition - Connectionless-Mode Presentation Service
ISO 9576◆	Presentation Connectionless Protocol to Provide Connectionless-Mode Presentation Service (X.236)
DIS 9576-2◆	Presentation Protocol to Provide the Connectionless-Mode Presentation Service, Part 2: PICS Proforma for Connectionless Presentation Protocol (X.256)
ITU-TS X.236	Connectionless-Mode Presentation Protocol: Protocol Specification (ISO 9576), Draft, 1993
ITU-TS X.256	Connectionless-Mode Presentation Protocol: PICS Proforma (ISO 9576-2), Draft, 1993

C. ABSTRACT SYNTAX NOTATION ONE (ASN.1):

STANAG 4258◆	Specification of ASN.1
STANAG 4259◆	Specification of Basic Encoding Rules for ASN.1

24 The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

ISO/IEC 8824		Specification of Abstract Syntax Notation One (ASN.1) (X.208)
	DAM 2	Amendments to ISO 8824 to Give ISO 8824 Part 1: Specification of Basic Notation
	WDAM 4	Removal of Definition of Root Arcs of Object Identifier Tree
	Cor 1	Draft Technical Corrigendum 1
ISO/IEC 8824-1		Specification of Abstract Syntax Notation One (ASN.1), Part 1: Specification of Basic Notation (X.680)
	PDAM 3.2	Rules of Extensibility
ISO/IEC 8824-2		Specification of Abstract Syntax Notation One (ASN.1), Part 2: Information Object Specification (X.681)
ISO/IEC 8824-3		Specification of Abstract Syntax Notation One (ASN.1), Part 3: Constraint Specification (X.682)
ISO/IEC 8824-4		Specification of Abstract Syntax Notation One (ASN.1), Part 4: Parameterization of ASN.1 Specifications (X.683)
ISO/IEC 8825		Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) (X.209)
	DAM 2	Amendments to ISO 8825 to Give ISO 8825 Part 1: Basic Encoding Rules
	AM 3	Rules for Extensibility
	Cor 1	Draft Technical Corrigendum 1
DIS 8825-1		Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 1: Basic Encoding Rules (BER) (X.690)
	WDAM 1	Light Weight Encoding Rules for ASN.1
DIS 8825-2.2		Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 2: Packed Encoding Rules (PER)
DIS 8825-3		Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 3: Distinguished and Canonical Encoding Rules (X.692)
DIS 8825-4		Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 4: Test Suite Structure and Test Purposes for ASN.1 Encodings
SC21 N 6130		Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression
ITU-TS X.208		Specification of Abstract Syntax Notation One (ASN.1), 1988 (see X.680)
ITU-TS X.209		Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), 1988 (see X.690)
ITU-TS X.680		ASN.1: Specification of Basic Notation, Basic ASN.1 (ISO 8824-1), Draft, 1993
ITU-TS X.681		ASN.1: Information Object Specification (ISO 8824-2), Draft, 1993
ITU-TS X.682		ASN.1: Constraint Specification (ISO 8824-3), Draft, 1993
ITU-TS X.683		ASN.1: Parameterization of ASN.1 Specifications (ISO 8824-4), Draft, 1993
ITU-TS X.690		Specification of ASN.1 Encoding Rules: Basic Encoding Rules (ISO 8825-1), Draft, 1993
ITU-TS X.691		Specification of ASN.1 Encoding Rules: Packet Encoding Rules (ISO 8825-1), Draft, 1993
ITU-TS X.692		Specification of ASN.1 Encoding Rules: Distinguished and Canonical Encoding Rules (ISO 8825-3), Draft, 1993

D. TELEMATIC SERVICES:

ITU-TS T.6	Facsimile (FAX) Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus
ITU-TS T.51	Coded Character Sets for Telematic Services
ITU-TS T.61 Rev 1	Character Repertoire and Coded Character Sets for the International Teletex Service
ITU-TS T.73	Document Interchange Protocol for the Telematic Services

VIII. LAYER 7: APPLICATION LAYER[25]

A. GENERAL:

ISO/IEC 9545◆	Application Layer Structure (ALS),1993 (includes XALS) (X.207)
ISO/IEC 10745	Upper Layer Security Model
SC21 N 6017	Comments on Standardization of Application Programmatic (sic) Interfaces
SC21 N 6797	Comments on SC21 N 6068, Modelling Recovery in the Application Layer
SC21 N 6967	Modelling Recovery in the Application Layer
SC21 N 6970	Call for Comments on the Progression of the ALS Extension to Cover Connectionless Mode of Communications
SC21 N 6971	Application of XALS Concepts to Specification of Mappings
SC21 N 7209	Initial SC21 Considerations in Support of the Initiation of a Study Period on Application Programmatic Interfaces
SC21 N 7902	Methodology and Guidelines for the Development of Application Layer Standards
SC21 N 8019	Liaison Statement to ITU-TS/SG7 on Q1/67 - Generalization of ASO Concept, SC21/WG1, August 1993
SC21 N 8330	Version V2 of the APA-Application Standard, ECMA/TC-TG9, November 1993
SC21 N 8410	Methodology and Guidelines for the Development of Application Layer Protocols
ITU-TS X.207	Application Layer Structure (ISO 9545), Draft, 1993

B. OSI DIRECTORY:

ISO/IEC 9594-1◆	The Directory, Part 1: Overview of Concepts, Models and Services (X.500)
AM 1◆	Replication, Schema and Access Control
WD 9594-1/9 WDAMs	Amendments to Parts 1 to 9 on Internationalization of the Directory Enhancement of Directory

[25] The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

WD 9594-1/9 WDAMs	Amendments to Parts 1 to 9 on Enhancement of Directory Operational Security		
WD 9594-1/9 WDAMs	Amendments to Parts 1 to 9 on Directory Schema Migration		
DIS 9594-1.2	The Directory, Part 1: Overview of Concepts, Models and Services, Edition 2 (X.500)		
ISO/IEC 9594-2•	The Directory, Part 2: Models (X.501)		
		AM 1•	Access Control
		AM 2	Schema Extensions
		AM 3	Replication
		Cor 1-2	Technical Corrigenda 1-2
DIS 9594-2.2	The Directory, Part 2: Models, Edition 2 (X.501)		
ISO/IEC 9594-3•	The Directory, Part 3: Abstract Service Definition (X.511)		
		AM 1•	Access Control
		AM 2	Replication, Schema and Enhanced Search
		Cor 1-4	Technical Corrigenda 1-4
ISO 9594-3.2	The Directory, Part 3: Abstract Service Definition, Edition 2 (X.511)		
ISO/IEC 9594-4•	The Directory, Part 4: Procedures for Distributed Operations (X.518)		
		AM 1•	Access Control
		AM 2	Replication, Schema and Enhanced Search
		Cor 1-3	Technical Corrigenda 1-3
ISO 9594-4.2	The Directory, Part 4: Procedures for Distributed Operations, Edition 2 (X.518)		
ISO/IEC 9594-5•	The Directory, Part 5: Protocol Specifications (X.519)		
		AM 1•	Replication
		Cor 1	Technical Corrigendum 1
ISO 9594-5.2	The Directory, Part 5: Protocol Specifications, Edition 2 (X.519)		
ISO/IEC 9594-6•	The Directory, Part 6: Selected Attribute Types (X.520)		
		AM 1•	Schema Extensions
ISO 9594-6.2	The Directory, Part 6: Selected Attribute Types, Edition 2 (X.520)		
ISO/IEC 9594-7•	The Directory, Part 7: Selected Object Classes (X.521)		
		AM 1•	Schema Extensions
		Cor 1-2	Technical Corrigenda 1-2
ISO 9594-7.2	The Directory, Part 7: Selected Object Classes, Edition 2 (X.521)		
ISO/IEC 9594-8•	The Directory, Part 8: Authentication Framework (X.509)		
		AM 1•	Access Control
		WDAM	Security Enhancement to Directory
		Cor 1	Technical Corrigendum 1
DIS 9594-8.2	The Directory, Part 8: Authentication Framework, Edition 2 (X.509)		
ISO/IEC 9594-9	The Directory, Part 9: Replication (X.525)		
CD 9594-10•	The Directory, Part 10: Directory PICS Proforma DUA PICS Proforma (X.581)		
WD 9594-11	The Directory, Part 11: Directory PICS Proforma DSA PICS Proforma (X.582)		
WD 9594-w	The Directory, Part w: Use of Systems Management for Administration of Directory		
DISP 10615-1•	ISPs ADI nn -- OSI Directory, Part 1: ADI 11, DUA Support of Directory Access, January 1993		
DISP 10615-2•	ISPs ADI nn -- OSI Directory, Part 2: ADI 12, DSA Support of Directory Access, January 1993		
DISP 10615-3•	ISPs ADI nn -- OSI Directory, Part 3: ADI 21, DSA Responder Role, July 1993		
DISP 10615-4•	ISPs ADI nn -- OSI Directory, Part 4: ADI 22, DSA Initiator Role, July 1993		
pDISP 10615-5	ISPs ADI nn -- OSI Directory, Part 5: ADI 31, DUA Support of Distributed Operations, 1993		
pDISP 10615-6	ISPs ADI nn -- OSI Directory, Part 6: ADI 32, DSA Support of Distributed Operations, 1993		
pDISP 10615-7	ISPs ADI nn -- OSI Directory, Part 7: ADI 41, Strong Authentication, 1993		
SC21 N 6821	Internationalization of the Directory		
SC21 N 6822	UK Response to N 6011, Call for Contributions on Directory Enhancements		
SC21 N 6842	US Concerns Regarding the Ballot Responses on the Authentication Service NP and Enhancements to Directory Authentication NP		
SC21 N 6872	Liaison Statement to CCITT Q20/VII and SC21/WG4 from SC18 on MHS Use of Directory		
SC21 N 6975	Need for Procedures to Coordinate the Definition and Extension of Directory Objects		
SC21 N 7018	Use of Systems Management for Administration of the Directory		
SC21 N 7020	Enhancement of Directory Operational Security		
SC21 N 7021	Registration of Question Q4/4 on Directory Schema Migration, Including Disposition of Comments		
SC21 N 7024	Request for Contributions on Use of Systems Management for Administration of the Directory		
SC21 N 7025	Request for Contributions on Movement of Directory Information by Means Other Than Directory Protocols		
SC21 N 7026	Request for Comments on the Need for an Extension to the Directory Standard to Support Extended Relationships Among Directory Entries		
SC21 N 7028	Status of Directory Defects		
SC21 N 7102	Extensions to ISO/IEC 9594-8 (Certificate Definitions)		

SC21 N 7116	Working Document on Complex Attribute Types
SC21 N 7566	Directory Implementor's Guide, Version 7
SC21 N 7930	Working Document on Use of OSI System Management for the Administration of the Directory
SC21 N 7931	Working Document on the Internationalization of the Directory
SC21 N 7932	Enhancement of Directory Operational Security
SC21 N 8315	Question on Registration of Names of International Organizations for Directory, USA, October 1993
SC21/WG4 N 1527	Closing WG4 Plenary Report on Directory Meeting, Ottawa
ITU-TS X.500	The Directory: Overview of Concepts, Models, and Services (ISO 9594-1), 1988
ITU-TS X.501	The Directory: Models (ISO 9594-2), 1988
ITU-TS X.509	The Directory: Authentication Framework (ISO 9594-8), 1988
ITU-TS X.510	Overview of Sub-series T.510 Recommendations
ITU-TS X.511	The Directory: Abstract Service Definition (ISO 9594-3), 1988
ITU-TS X.518	The Directory: Procedures for Distributed Operation (ISO 9594-4), 1988
ITU-TS X.519	The Directory: Protocol Specifications (ISO 9594-5), 1988
ITU-TS X.520	The Directory: Selected Attribute Types (ISO 9594-6), 1988
ITU-TS X.521	The Directory: Selected Object Classes (ISO 9594-7), 1988
ITU-TS X.525	The Directory: Replication (ISO 9594-9)
ITU-TS X.581	The Directory: DUA PICS Proforma (ISO 9594-10)
ITU-TS X.582	The Directory: DSA PICS Proforma (ISO 9594-10)

C. OPERATING SYSTEM INTERFACE:

ISO 2375	Data Processing - Procedures for the Registration of Escape Sequences
ISO 9945-1	Portable Operating System Interface for Computer Environments (POSIX), Part 1: System Interface
CD 9945-1.1	Portable Operating System Interface for Computer Environments (POSIX), Part 1.1: Language Independent Base
CD 9945-1.2	Portable Operating System Interface for Computer Environments (POSIX), Part 1.2: Real-time and Extensions
CD 9945-1.3	Portable Operating System Interface for Computer Environments (POSIX), Part 1.3: Distribution Services
CD 9945-1.3.1	Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.1: Transparent File Access
CD 9945-1.3.2	Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.2: Remote Procedure Call
CD 9945-1.3.3	Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.3: Transport Interface
CD 9945-1.3.4	Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.4: Name Space/Directory Services
DIS 9945-2.1	Portable Operating System Interface for Computer Environments (POSIX), Part 2.1: Shell and Utilities
CD 9945-2.2	Portable Operating System Interface for Computer Environments (POSIX), Part 2.2: User Portability Extensions
CD 9945-3	Portable Operating System Interface for Computer Environments (POSIX), Part 1: System Management
CD 9945-3.1	Portable Operating System Interface for Computer Environments (POSIX), Part 3.1: General Services
CD 9945-3.2	Portable Operating System Interface for Computer Environments (POSIX), Part 3.2: Batch Services
SC21 N 6403	Proposal for a New Work Item: Generic Operating System Interface

D. ASSOCIATION CONTROL SERVICE ELEMENT (ACSE):

ISO 8649:1988◆	Service Definition for the ACSE (X.217)	
ISO 8649:1992	Service Definition for the ACSE, Revised Edition (X.217)	
	DAM 3◆	Application Context Management Service
	WDAM 4	Extensions to Support the Extended Application Layer Structure
DIS 8649.2◆	Service Definition for the Association Control Service Element (ACSE), Edition 2	
ISO 8650:1988◆	Protocol Specification for the ACSE (X.227)	
ISO 8650:1992	Protocol Specification for the ACSE, Revised Edition (X.227)	
	DAM 2◆	Application Context Negotiation During Association Establishment
	WDAM 3	Application Context Management Service
	WDAM 4	Extensions to Support the Extended Application Layer Structure
	Cor 2	Technical Corrigendum 2

DIS 8650-1	Protocol Specification for the Association Control Service Element (ACSE), Edition 2 of ISO 8650
ISO 8650-2♦	Protocol Specification for the (ACSE) Part 2: PICS Proforma (X.247)
ISO 10035♦	Connectionless ACSE Protocol Specification (X.237)
	WDAM 1 Extensions to Support the Extended Application Layer Structure
DIS 10035-2	Connectionless ACSE Protocol Specification, Part 2: PICS Proforma for Connectionless ACSE Protocol
ISO/IEC 10169-1♦	Conformance Test Suite for the ACSE Protocol, Part 1: Test Suite Structure and Test Purposes
WD 10169-2	Conformance Test Suite for the Session Protocol, Part 2: Common ACSE Abstract Test Suite
SC21 N 6796	US Response on Application Context Negotiation
SC21 N 6798	US Request for Extensions to ACSE
SC21 N 7014	ACSE Enhancements Covering ASOs and ASO-associations
SC21 N 7092	Proposed New Question Q1/67 on Generalization of ASO Concepts
ITU-TS X.217	Service Definition for the Association Control Service Element (ISO 8649), 1992
ITU-TS X.227	Protocol Specification for the Association Control Service Element (ISO 8650), 1992
ITU-TS X.237	Connectionless-Mode Protocol Specification for the Association Control Service Element (ISO 10035), 1992
ITU-TS X.247	Connection-Mode Protocol Specification for the Association Control Service Element: PICS Proforma (ISO 8650-2), Draft, 1993
ITU-TS X.257	Connectionless-Mode ACSE Protocol: PICS Proforma (ISO 10035-2), Draft, 1993

E. COMMITMENT, CONCURRENCY, AND RECOVERY (CCR) SERVICE ELEMENT:

ISO/IEC 9804♦	Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element (X.851)
	PDAM 1.2 Enhancements
	AM 2 Session Mapping Changes (Additional Resynchronization Functionality)
	WDAM 3 Restart
	Cor 1 Technical Corrigendum 1
DIS 9804.2	Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element, Edition 2, (X.851)
ISO/IEC 9805♦	Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element Protocol (X.852)
	PDAM 1.2 Enhancements
	AM 2 Session Mapping Changes (Additional Resynchronization Functionality)
	WDAM 3 Restart
	Cor 1-2 Technical Corrigenda 1-2
ISO/IEC 9805-1:1993	Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service Element Protocol, Edition 2 of ISO/IEC 9805, 1993 (X.852)
DIS 9805-2.2♦	Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Protocol, Part 2: PICS Proforma (X.853)
PDTR 11589	LOTOS Description of the CCR Service, 1993
PDTR 11590	LOTOS Description of the CCR Protocol, 1993
SC21 N 7335	Working Draft for LOTOS Description of the CCR Protocol
SC21 N 7336	Working Draft for LOTOS Description of the CCR Service
ITU-TS X.851	Service Definition of CCR Service Element, Edition 2 (ISO 9804), Draft, 1993
ITU-TS X.852	CCR Service Element: Protocol Specification (ISO 9805-1), Draft, 1993
ITU-TS X.853	CCR Service Element: PICS Proforma, Edition 2 (ISO 9805-2), Draft, 1993

F. RELIABLE TRANSFER (RT), REMOTE OPERATIONS (RO), AND REMOTE PROCEDURE CALL (RPC):

ISO/IEC 9066-1♦	Reliable Transfer (RT), Part 1: Model, Notation and Service Definition
ISO/IEC 9066-2♦	Reliable Transfer (RT), Part 2: Protocol Specification
	Cor 1 Technical Corrigendum 1
DIS 9066-3	Reliable Transfer (RT), Part 3: PICS Proforma
ISO 9072-1:1989♦	Remote Operations (RO), Part 1: Model, Notation and Service Definition, Edition 2
	PDAM 1 Enhancements to Service Definition
ISO/IEC 9072-1:1993♦	Remote Operations (RO), Part 1: Concepts, Model, and Notation, Edition 3 (see DIS 13712-2)
	PDAM 1 Built-In Operations
ISO 9072-2:1989♦	Remote Operations (RO), Part 2: Protocol Specification, Edition 2
	PDAM 1 Enhancements to Protocol Specification
ISO/IEC 9072-2:1993♦	Remote Operations (RO), Part 2: Service Definition, Edition 3 (see DIS 13712-2)
	PDAM 1 Mapping to A-UNITDATA and Built-In Operations

ISO/IEC 9072-3:1993	Remote Operations (RO), Part 3: Protocol Specification
	PDAM 1 Mapping to A-UNITDATA and Built-In Operations
DIS 9072-4	Remote Operations (RO), Part 4: PICS Proforma
WD 10148.3	Basic Remote Procedure Call (RPC) Using OSI Remote Operations
pDISP 11188-1	ISPs - Common Upper Layer Requirements, Part 1: Basic Connection Oriented Requirements, 1993
pDISP 11188-2	ISPs - Common Upper Layer Requirements, Part 2: ROSE Based Requirements, 1993
pDISP 11188-3	ISPs - Common Upper Layer Requirements, Part 3: Minimal OSI Upper Layer Facilities, July 1993
DIS 11578-1•	Remote Procedure Call (RPC), Part 1: Model
DIS 11578-2•	Remote Procedure Call (RPC), Part 2: Interface Definition Notation
DIS 11578-3•	Remote Procedure Call (RPC), Part 3: Service Definition
DIS 11578-4•	Remote Procedure Call (RPC), Part 4: Protocol Specification
WD 11578-5	Remote Procedure Call (RPC), Part 5: PICS Proforma
DIS 13712-1	Remote Operations (RO), Part 1: Model, 1993 (X.880)
	PDAM 1 Built-In Operations, January 1994
DIS 13712-2	Remote Operations (RO), Part 2: Service, 1993 (X.881)
	PDAM 1 Mapping to A-UNITDATA and Built-In Operations, January 1994
DIS 13712-3	Remote Operations (RO), Part 3: Protocol, 1993 (X.882)
	PDAM 1 Mapping to A-UNITDATA and Built-In Operations, January 1994
DIS 13712-4	Remote Operations (RO), Part 4: PICS Proforma, 1993 (X.883))
WD 13712-5	Remote Operations (RO), Part 5: Enhancements, 1993
SC21 N 5593	The Role of the Extended Application Layer Structure in the Standardization of RPC, ECMA
SC21 N 5817	Binding Concepts Within RPC, ECMA
SC21 N 5819	Modelling Rationale for OSI RPC, ECMA
SC21 N 6638	Issues for National Body and Liaison Organization Comment on RPC
SC21 N 6719	Recommendations of the CCITT and ISO Collaborative Interim Meeting Covering ROSE Enhancements
SC21 N 6722	Issues Concerning Mapping of ROSE APDUs onto A-UNIT-DATA
SC21 N 6723	Enhancement to ROSE, Part 3: Concepts, Model and Notation
SC21 N 6724	Enhancement to ROSE, Part 1: Service Definition
SC21 N 6725	Enhancement to ROSE, Protocol Definition
SC21 N 6880	Liaison Statement to CCITT Q19/VII and SC21/WG6 from SC18 on Reliable Transfer Service Element (RTSE)
SC21 N 6904	Liaison Statement to SC21 on Mapping of ROSE APDUs onto the A-UNIT-DATA Service
SC21 N 7011	Liaison Statement to SC18 on Compatibility of ROSE and RPC SC21/WG6
SC21 N 7013	Enhancement to ROSE Concepts, Model and Notation, ROSE Service Definition and Protocol Specification
SC21 N 8270	Liaison Statement to SC21 WG/8 on the ROSE Standard, ITU-TS SG7, October 1993
ITU-TS X.218 Rev 1	Reliable Transfer: Model and Service Definition (ISO 9066-1), 1993
ITU-TS X.219	Remote Operations: Model, Notation and Service Definition (ISO 9072-1), 1988 (see X.880, X.881)
ITU-TS X.228	Reliable Transfer: Protocol Specification (ISO 9066-2), 1988
ITU-TS X.229	Remote Operations: Protocol Specification (ISO 9072-2), 1988 (see X.882)
ITU-TS X.248	Reliable Transfer Service Element - PICS Proforma, 1992
ITU-TS X.249	Remote Operations Service Element - PICS Proforma, 1992 (see X.883)
ITU-TS X.880	Remote Operations (RO), Part 1: Model, 1993 (CD 13712-1), Draft, 1993
ITU-TS X.881	Remote Operations (RO), Part 2: Service, 1993 (CD 13712-2), Draft, 1993
ITU-TS X.882	Remote Operations (RO), Part 3: Protocol, 1993 (CD 13712-3), Draft, 1993
ITU-TS X.883	Remote Operations (RO), Part 4: PICS Proforma, 1993 (CD 13712-4), Draft, 1993

G. MESSAGE HANDLING SYSTEM (MHS):

STANAG 4406• Military Message Handling System, Draft, NATO UNCLASSIFIED (cf. ISO 10021, 10611)

- Main Body, Draft
- Annex A—MMHS Extensions to ISO 10021 Series, Draft
- Annex B—Security Aspects of MMHS (under development)
- Annex C—Alpha Profile Set (a delta specification to EWOS profiles): AMH1x(M) on Common Facilities and AMH9x(M) on Military Messaging, Draft
- Annex D—Alpha/ACP 127 Gateway (under development)
- Annex E—Alpha/MMHS(84) Gateway (under development)
- Annex F—Alpha/MHS(88) Gateway (under development)
- Annex G—Beta Profile Set (under development)
- Annex H—Beta/ACP 127 Gateway (under development)
- Annex I—Beta/Alpha Gateway (under development)

DISP 10611-1•	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 1: Service Support, 1993
DISP 10611-2•	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 2: Specification of ROSE, RTSE, ACSE, Presentation, and Session for Use by MHS, 1993
DISP 10611-3•	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 3: AMH11: Message Transfer (P1), 1993
DISP 10611-4•	ISPs AMH1n - Message Handling Systems - Common Messaging, Part 4: AMH12: MTS Access (P2), 1993
DISP 10611-5•	ISPs AMH1n - Message Handling Systems - Common Messaging, Parat 5: AMH13: MS Access (P7), 1993
pDISP 12062-1	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 1: IPM MHS Service Support, August 1993 (review ended December 1993)
pDISP 12062-2	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 2: AMH 21, IPM Content, August 1993 (review ended December 1993)
pDISP 12062-3	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 3: AMH 22, IPM Requirements for Message Transfer (P1), August 1993 (review ended December 1993)
pDISP 12062-4	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 4: AMH 23, IPM Requirements for MTS Access (P3), August 1993 (review ended December 1993)
pDISP 12062-5	International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 5: IPM Requirements for Enhanced MS Access (P7), August 1993 (review ended December 1993)
pDISP 12063	International Standardized Profiles AMH 3 - Message Handling Systems, 1993
ITU-TS F.400	Message Handling System and Service Overview
ITU-TS F.401	Naming and Addressing for Public Message Handling Services
ITU-TS F.410	The Public Messaging Transfer Service
ITU-TS F.415	Intercommunication with Public Physical Delivery Services
ITU-TS F.420	The Public Interpersonal Messaging (IPM) Service
ITU-TS F.421	Intercommunication Between the IPM Service and the Telex Service
ITU-TS F.422	Intercommunication Between the IPM Service and the Teletex Service
ITU-TS F.435	Message Handling: EDI Messaging Service
ITU-TS F.500	International Public Directory Services
ITU-TS X.400/F.400 Rev 1	Message Handling Systems (MHSs): Message Handling System and Service Overview (ISO 10021-1), 1993 (approval target for common text with ISO/IEC November 1994)
ITU-TS X.401	MHSs - Basic Service Elements and Optional User Facilities, 1984 (discontinued)
ITU-TS X.402	MHSs - Overall Architecture (ISO 10021-2), 1992 (approval target for common text with ISO/IEC November 1994)
ITU-TS X.403	MHSs - Conformance Testing, 1988
ITU-TS X.407	MHSs - Abstract Service Definition Conventions (ISO 10021-3), 1988 (approval target for revision and common text with ISO/IEC November 1994)
ITU-TS X.408	MHSs - Encoded Information-Type Conversion Rules, 1988
ITU-TS X.409	MHSs - Presentation Transfer Syntax and Notation, 1984 [replaced by ITU-TS X.208 (ISO 8824 with DAD 1) and ITU-TS X.208 (ISO 8825 with DAD 1)] (discontinued)
ITU-TS X.410	MHSs - Remote Operations and Reliable Transfer Server, 1984 [replaced by ITU-TS X.218 (ISO 9066-1), ITU-TS X.219 (ISO 9072-1), ITU-TS X.228 (ISO 9066-2), and ITU-TS X.229 (ISO 9072-2)] (discontinued)
ITU-TS X.411	MHSs - Message Transfer System: Abstract Service Definition and Procedures (ISO 10021-4), 1992 (approval target for common text with ISO/IEC November 1994)
ITU-TS X.413	MHSs - Message Store: Abstract Service Definition (ISO 10021-5), 1992 (approval target for common text with ISO/IEC November 1994)
ITU-TS X.419	MHSs - Protocol Specifications (ISO 10021-6), 1992 (approval target for common text with ISO/IEC November 1994)
ITU-TS X.420	MHSs - Interpersonal Messaging Sysem (ISO 10021-7), 1992 (approval target for common text with ISO/IEC November 1994)
ITU-TS X.421	COMFAX Use of MHS, Draft, 1993 (approval target February 1994)
ITU-TS X.435	Message Handling Systems: Electronic Data Interchange (EDI) Messaging System, 1991 (fast-track balloting in ISO/IEC)
ITU-TS X.440	Message Handling Systems: Voice Messaging System, 1992
ITU-TS X.480	Message Handling Systems and Directory Services Conformance Testing, 1992
ITU-TS X.481	MHSs - P2 Protocol: PICS Proforma, 1992
ITU-TS X.482	MHSs - P1 Protocol: PICS Proforma, 1992
ITU-TS X.483	MHSs - P3 Protocol: PICS Proforma, 1992
ITU-TS X.484	MHSs - P7 Protocol: PICS Proforma, 1992
ITU-TS X.485	MHSs - Voice Messaging System PICS Proforma, 1992

ITU-TS X.4acc	Information Technology - Communication - Message Handling System (MHS): Computer Conferencing, Draft, 1993
ITU-TS X.4ae	MHS Management: Access Unit Entity, Draft, 1993 (approval target 1995-1996)
ITU-TS X.4agc	Information Technology - Communication - Message Handling System (MHS): Group Communication, Draft, 1993
ITU-TS X.4cm	MHS Management: Configuration Management Function, Draft, 1993 (approval target 1995-1996)
ITU-TS X.ep	Information Technology - Message Handling Systems - PICS Proforma for EDIMG, Draft, 1993 (approval target November 1994)
ITU-TS X.4fm	MHS Management: Fault Management Function, Draft, 1993 (approval target 1995-1996)
ITU-TS X.4gm/ITU-TS X.inf	MHS Management: Information and Functional Overview, Draft, 1993 (approval target 1995-1996)
ITU-TS X.4ma	MHS Management: Accounting Management, Draft, 1993 (approval target November 1994)
ITU-TS X.4me	MHS Management: Message Store Entity, Draft, 1993 (approval target 1995-1996)
ITU-TS X.4mma	MHS Management: Model and Architecgture, Draft, 1993 (approval target November 1994)
ITU-TS X.4mo	MHS Management: MTA Management, Draft, 1993 (approval target 1995)
ITU-TS X.4pm	MHS Management: Performance Management Function, Draft, 1993 (approval target 1995-1996)
ITU-TS X.4sm	MHS Management: Security Management, Draft, 1993 (approval target June 1995)
ITU-TS X.4ue	MHS Management: User Agent Entity, Draft, 1993 (approval target 1995-1996)

H. MESSAGE ORIENTED TEXT INTERCHANGE SYSTEM (MOTIS):[26]

DIS 8505	Functional Description and Service Specification for Message Oriented Text Interchange Systems	
DIS 8883	Message Oriented Text Interchange System, Message Transfer Sublayer, Message Interchange Service and Message Transfer Protocol	
DIS 9065	Message Oriented Text Interchange System (MOTIS) User Agent Sublayer - Interpersonal Messaging User Agent - Message Interchange Formats and Protocols	
ISO/IEC 10021-1◆	MOTIS - Part 1: System and Service (X.400)	
	Cor 1-5	MOTIS, Technical Corrigenda 1-5
ISO/IEC 10021-2◆	MOTIS - Part 2: Overall Architecture (X.402)	
	PDAM 1	Representation of O/R Addresses for Human Exchange
	PDAM 2	Minor Enhancements
	Cor 1-4	MOTIS, Technical Corrigenda 1-4
ISO/IEC 10021-3◆	MOTIS - Part 3: Abstract Service Definition Conventions (X.407)	
	Cor 1	MOTIS, Technical Corrigendum 1
ISO/IEC 10021-4◆	MOTIS, Part 4: Message Transfer System - Abstract Service Definition and Procedures (X.411)	
	PDAM 1	Minor Enhancements
	Cor 1-5	MOTIS, Technical Corrigenda 1-5
ISO/IEC 10021-5◆	MOTIS - Part 5: Message Store - Abstract Service Definition (X.413)	
	Cor 1-5	MOTIS, Technical Corrigenda 1-5
ISO/IEC 10021-6◆	MOTIS - Part 6: Protocol Specifications (X.419)	
	Cor 1-5	MOTIS, Technical Corrigenda 1-5
ISO/IEC 10021-7◆	MOTIS - Part 7: Interpersonal Message System (X.420)	
	PDAM 1	Minor Enhancements
	Cor 1-5	MOTIS, Technical Corrigenda 1-5
ISO/IEC 10021-11	MOTIS - Part 11: MTS Routing	
ISO/IEC 10021-12	MOTIS - Part 12: PICS Proforma for Message Transfer Protocol	
ISO/IEC 10021-13	MOTIS - Part 13: PICS Proforma for Message Transfer Access Protocol	
ISO/IEC 10021-14	MOTIS - Part 14: PICS Proforma for Message Store Access Protocol	
ISO/IEC 10021-15	MOTIS - Part 15: PICS Proforma for Interpersonal Messaging	
ISO 10538	Control Functions for Text Communication	
SC21 N 7144	Liaison Statement to SC18 Concerning Mapping of Systems Management Object Management Function onto MOTIS	

I. MANUFACTURING MESSAGE SPECIFICATION:

ISO 9506-1	Manufacturing Message Specification, Part 1: Service Definition	
	AD 1	Data Exchange, 1993
ISO 9506-2	Manufacturing Message Specification, Part 2: Protocol Specification	
	AD 1	Data Exchange, 1993
ISO 9506-3	Manufacturing Message Specification, Part 3: Companion Standard for Robotics	
ISO 9506-4	Manufacturing Message Specification, Part 4: Companion Standard for Numerical Control	

[26] DIS 8505◆, DIS 8883◆, and DIS 9065◆ have been superceded by the other standards.

J. FILE TRANSFER, ACCESS AND MANAGEMENT (FTAM):

ISO 8571-1•	FTAM, Part 1: General Introduction, Second Edition (incorporating all	
	AM 1	Filestore Management
	AM 2	Overlapped Access
	AM 3	Service Enhancement
	WDAM 4	Security Enhancement
	Cor 1	Technical Corrigendum 1
WD 8571-1.2	FTAM, Part 1: General Introduction, Edition 2	
ISO 8571-2•	FTAM, Part 2: Virtual Filestore Definition	
	AM 1	Filestore Management
	AM 2	Overlapped Access
	PDAM 3	Service Enhancement
	WDAM 4	Enhancement to FTAM Security Services (Project SUSPENDED)
	Cor 1	Technical Corrigendum 1
WD 8571-2.2	FTAM, Part 2: Virtual Filestore Definition, Edition 2	
ISO 8571-3•	FTAM, Part 3: File Service Definition	
	AM 1	Filestore Management
	AM 2	Overlapped Access
	AM 3	Service Enhancement
	WDAM 4	Security Enhancement (Project SUSPENDED)
	Cor 1-2	Technical Corrigenda 1-2
WD 8571-3.2	FTAM, Part 3: File Service Definition, Edition 2	
ISO 8571-4•	FTAM, Part 4: File Protocol Specification	
	AM 1	Filestore Management
	AM 2	Overlapped Access
	AM 3	Service Enhancement
	AM 4	Defect Report Changes
	WDAM 5	Security Enhancement (Project SUSPENDED)
	Cor 1	Technical Corrigendum 1
WD 8571-4.2	FTAM, Part 4: File Protocol Specification, Edition 2	
ISO 8571-5•	FTAM, Part 5: Protocol Implementation Conformance Statement Proforma	
	PDAM 1	Filestore Management
	WDAM 2	Overlapped Access (project under reassessment)
	WDAM 3	Service Enhancement (to be progressed as a Technical Corrigenda)
	WDAM 4	Security Enhancement (Project SUSPENDED)
WD 8571-5.2	FTAM, Part 5: Protocol Implementation Conformance Statement Proforma, Edition 2	
ISO/IEC 10170-1•	Conformance Test Suite for the FTAM Protocol, Part 1: Test Suite Structure and Test Purposes	
WD 10170-2	Conformance Test Suite for the FTAM Protocol, Part 2: FTAM Abstract Test Suite	
WD 10170-3	Conformance Test Suite for the FTAM Protocol, Part 3: ACSE Abstract Test Suite Embedded Under FTAM	
WD 10170-4	Conformance Test Suite for the FTAM Protocol, Part 4: Presentation Abstract Test Suite Embedded Under FTAM	
WD 10170-5	Conformance Test Suite for the FTAM Protocol, Part 5: Session Abstract Test Suite Embedded Under FTAM	
ISO/IEC ISP 10607-1•	ISPs AFT nn - File Transfer, Access, and Management, Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM	
	DAM 1	Additional Specifications for COBOL Document Types
ISO/IEC ISP 10607-2•	ISPs AFT nn - File Transfer, Access, and Management, Part 2: Definition of Document Types, Constraint Sets and Syntaxes	
	DAM 1	Additional Definitions
	DAM 2	Additional Specifications for COBOL Document Types
	DAM 3	FTAM Constraint Set and Document Type for CGM
ISO/IEC ISP 10607-3•	ISPs AFT nn - File Transfer, Access, and Management, Part 3: AFT 11 - Simple File Transfer Service (Unstructured)	
ISO/IEC ISP 10607-4•	ISPs AFT nn - File Transfer, Access, and Management, Part 4: AFT 12 - Positional File Transfer Service	
	DAM 1	Additional Specifications for COBOL Document Types
ISO/IEC ISP 10607-5•	ISPs AFT nn - File Transfer, Access, and Management, Part 5: AFT 22 - Positional File Access Service	
	DAM 1	Additional Specifications for COBOL Document Types
ISO/IEC ISP 10607-6•	ISPs AFT nn - File Transfer, Access, and Management, Part 6: AFT 12 - File Management Service	
ISO/IEC ISP 10607-x	ISPs AFT nn - File Transfer, Access and Management, Part x: AFT 13 - Full File Transfer (Hierarchical), Draft, 1993	

ISO/IEC ISP 10607-y	ISPs AFT nn - File Transfer, Access and Management, Part y: AFT 23 - Full File Access (Hierarchical), Draft, 1993
ISO/IEC ISP 10607-z	ISPs AFT nn - File Transfer, Access and Management, Part z: AFT 4 - Filestore Management Profiles, Draft, 1993
SC21 N 6224	Proposed EDIFACT/FTAM Document Type
SC21 N 6225	Response to Liaison from JTC1/SC24/WG3 about CGM Document Types
SC21 N 6802	Problems with Certifying FTAM Implementation as Conformant
SC21 N 6811	FTAM Aspects of Security
SC21 N 6879	Liaison Statement to SC21/WG6 FTAM from SC18 on MHS File Transfer Body Part Type
SC21 N 6984	Class of Mappings from a Single ASN.1 Type to an FTAM Document Type
SC21 N 7160	FTAM Security Issues
SC21 N 7162	Status of Project JTC1.21.12.08.02, FTAM Virtual Filestore Service Enhancements
SC21 N 8256	Liaison Statement Regarding FTAM Abstract Test Suites, EWOS/EG FT, October 1993
SC21 N 8356	Draft Technical Corrigenda to ISO 8571, FTAM
SC21/WG 6 N 1159	Proposal for a New Work Item on a Class of Mappings from a Single ASN.1 Type to an FTAM Document Type

K. VIRTUAL TERMINAL (VT):

ISO 9040•	Virtual Terminal Service - Base Class	
	AM 2•	Additional Functional Units
	Cor 1-3	Technical Corrigenda 1-3
ISO 9041-1•	Virtual Terminal Protocol - Basic Class	
	AM 2•	Additional Functional Units
	Cor 1-2	Technical Corrigenda 1-2
ISO 9041-2•	Virtual Terminal (VT) Protocol, Part 2: VT PICS Proforma	
ISO/IEC 10739-1	Conformance Test Suite for 9041 - Virtual Terminal Basic Class Protocol, Part 1: Test Suite Structure and Test Purposes	
pDISP 11184-1	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 1: FVT 121, S-mode Forms VTE profile, 1993	
pDISP 11184-2	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 2: FVT 122, S-mode Paged VTE Profile, 1993	
pDISP 11184-3	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 3: FVT 111, A-mode Telnet Profile	
pDISP 11184-4	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 4: FVT 112, A-mode Scroll VTE Profile	
pDISP 11184-5	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 5: FVT 113, A-mode CCITT X.3 PAD Interworking	
pDISP 11184-6	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 6: FVT 114, A-mode Transparent VTE Profile	
pDISP 11184-7	ISPs FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 7: FVT 115, A-mode Generalized Telnet VTE Profile, 1993	
pDISP 11185-1	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 1: FVT 211, FVT 212, Sequenced and Unsequenced Application Control Objects, 1993	
pDISP 11185-2	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 2: FVT 213, FVT 214, Sequenced and Unsequenced Terminal Control Objects, 1993	
pDISP 11185-3	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 3: FVT 215, FVT 216, Application RIO Record Locating Control Object and Terminal RIO Record Notification Control Object, 1993	
pDISP 11185-4	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 4: FVT 217, Horizontal Tabulation Control Object, 1993	
pDISP 11185-5	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 5: FVT 218, Logical Image Control Object, 1993	
pDISP 11185-6	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 6: FVT 219, Status Message Control Object, 1993	
pDISP 11185-7	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 7: FVT 220, Entry-control Control Object, 1993	
pDISP 11185-8	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 8: FVT 221, Forms Field Entry Instruction Control Object (FEICO) No. 1, 1993	
pDISP 11185-9	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 9: FVT 222, Paged Field Entry Instruction Control Object (PEICO) No. 1, 1993	
pDISP 11185-10	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 10: FVT 231, Forms Field Entry Pilot Control Object (FEPCO) No. 1, 1993	
pDISP 11185-11	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 11: FVT 232, Paged Field Entry Pilot Control Object (PEPCO) No. 1, 1993	

pDISP 11185-12	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 12: FVT 251, Terminal Conditions Control Object No. 1
pDISP 11185-13	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 13: FVT 2111, Waiting Time Control Object (pDISP expected 1995)
pDISP 11185-14	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 14: FVT 2112, Printer Control Object, 1993
pDISP 11185-15	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 15: FVT 2113, Field Definition Control Object, 1993
pDISP 11185-16	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 16: FVT 2114, Terminal Signal Titles Control Object, 1993
pDISP 11185-17	ISPs FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 17: FVT 2115, Form Help Text Control Object, 1993
pDISP 11186-1	ISPs FVT 3nn - Virtual Terminal Basic Class - Register of Assignment Type Definitions, Part 1: FVT 321, Font Assignment Type No. 1
DISP 11187-1•	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 1: AVT 22, S-mode Forms Application Profile, 1993
DISP 11187-2•	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 2: AVT 23, S-mode Paged Application Profile, 1993
pDISP 11187-3	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 3: S-mode ISPICS Requirements List No. 1
pDISP 11187-4	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 4, S-mode ISPICS Requirements (IPRL) List No. 1, Supporting Layers List No. 1
pDISP 11187-6	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 6: AVT 13, A-mode Scroll Application Profile
pDISP 11187-7	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 7: AVT 14, A-mode CCITT X.3 PAD Application Profile
pDISP 11187-8	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 8: AVT 15, A-mode Transparent Application Profile
pDISP 11187-9	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 9: AVT 16, A-mode Generalized Telnet Application Profile, 1993
pDISP 11187-10	ISPs AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 10: AVT 17, A-mode ISPICS Requirements List No. 1

L. TERMINAL MANAGEMENT (TM), VISUAL DISPLAY TERMINAL (VDT), AND X-WINDOWS:

ISO 9241-1	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 1: Introduction
ISO 9241-2	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 2: General Guidance on Task Requirements
ISO 9241-3	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 3: Visual Display Requirements
DIS 9241-4	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 4: Keyboard Requirements
CD 9241-5	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 5: Workstation Layout and Postural Requirements
CD 9241-6	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 6: Environmental Requirements
CD 9241-7	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 7: Display Requirements with Reflections
CD 9241-8	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 8: Requirements for Displayed Colors
CD 9241-9	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 9: Requirements for Non-Keyboard Input Devices
WD 9241-10	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 10: Dialogue Principles
CD 9241-11	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 11: Usability Statements
CD 9241-12	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 12: Presentation of Information
WD 9241-13	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 13: User Guidance
CD 9241-14	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 14: Menu Dialogues
WD 9241-15	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 15: Command Dialogues
WD 9241-16	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 16: Direct Manipulation Dialogues

WD 9241-17	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 17: Form-Filling Dialogues
XX 9241-18	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 18: Question and Answer Dialogues
XX 9241-19	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 19: Natural Language Dialogues
CD 10184-1.2	Terminal Management - Model (project cancelled)
WD 10184-2	Terminal Management - Service (project cancelled)
WD 10184-3	Terminal Management - Protocol (project cancelled)
DIS 11730	Form Interface Management System (FIMS)
SC21 N 4189	Comments on the Integration of X-Windows into the OSI Environment

M. JOB TRANSFER AND MANIPULATION (JTM):

ISO/IEC 8831	Job Transfer and Manipulation Concepts and Services
ISO/IEC 8832	Specification of the Basic Class Protocol for Job Transfer and Manipulation

N. TELEMATIC SERVICES:

ITU-TS F.11	Continued Availability of Traditional Services
ITU-TS F.40	International Public Telemessage Service
ITU-TS F.41	Interworking Between the Telemessage Service and the International Public Telegram Service
ITU-TS F.59	General Characteristics of the International Telex Service
ITU-TS F.73	Operational Principles for Communication Between Terminals on Telex Networks and Data Terminal Equipment on Packet Switched Public Data Networks
ITU-TS F.80	Basic Requirements for Interworking Relations Between the International Telex Service and Other Services
ITU-TS F.82	Operational Provisions to Permit Interworking Between the International Telex Service and the INTEX Service
ITU-TS F.86	Interworking Between the International Telex Service and Videotex Service
ITU-TS F.87	Operational Principles for the Transfer of Messages from Terminals of the International Telex Service to Group 3 Facsimile Terminals Connected to the Public Switched Telephone Network
ITU-TS F.104	International Leased Circuit Services - Customer Circuit Designations
ITU-TS F.111	Principles of Service for Mobile Systems
ITU-TS F.150	Service and Operational Provisions for the INTEX Service
ITU-TS F.200	Teletex Service
ITU-TS F.200/C	Teletex Service, Annex C: Mixed Mode of Operation
ITU-TS F.201 Rev 1	Internetworking Between the Teletex Service and the Telex Service

O. INFORMATION RESOURCE DICTIONARY SYSTEM (IRDS):

DP 8800-1	Information Resource Dictionary System (IRDS), Part 1: Command Language and Panel Interface (project cancelled)
ISO/IEC 10027	IRDS Framework, June 1990
WD 10027.2	Information Resource Dictionary System (IRDS) Framework, Edition 2 (revision to address new requirements and alignment with RMDM, SQL, RDA, Directory, and ODP)
ISO/IEC 10728	IRDS - Services Interface PDAM 1 — C Language Binding WDAM 2 — Ada Language Binding
WD 10728-2	IRDS - Services Interface, Edition 2
SC21 N 6251	Proposed New Question on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM)
SC21 N 6252	Revision of the IRDS Framework
SC21 N 6253	Proposed New Question on the Approach to Remote IRDS Access
SC21 N 6257	Recommendation on NWI for Stored DBL Procedures
SC21 N 7178	Proposed NP for Guidelines for the Design of IRDS Content Modules
SC21 N 7181	Proposed Draft Answer to Question Q3/009 - Remote IRDS Access
SC21 N 7182	Liaison Statement to ECMA TC33 on IRDS/PCTE
SC21 N 7191	Liaison Statement to ISO TC184/SC5 on Reference Model and IRDS for Automation
SC21 N 7201	Amendment to ISO 10728 for C Language Binding
SC21 N 7203	IRDS Framework Revision
SC21 N 7486	Draft IRDS Conceptual Schema
SC21 N 8202	Working Draft of IRDS Services Interface Extensions

SC21 N 8204	Working Draft of IRDS Framework (Revision of ISO 10027:1990)
SC21/WG3 N 1279	Report of Meeting CDIF/1175/PDES Information Coordination
SC21/WG3 N 1283	IRDS Services Interface Extensions - Design Document
SC21/WG3 N 1406	Agreed Scope of Work for the Revision of the IRDS Framework (IS 10027), Ottawa

P. REMOTE DATABASE ACCESS (RDA):

ISO 9579-1◆	Remote Database Access (RDA), Part 1: Generic Model, Service, and Protocol WDAM 1 Generic RDA
ISO 9579-2◆	Remote Database Access (RDA), Part 2: SQL Specialization PDAM 1 Support for SQL2 WDAM 2 RDA Support for Shared DBL Statements
CD 9579-3	Remote Database Access (RDA), Part 3: SQL PICS Proforma
SC21 N 7177	Proposed New Work Item for Remote Database Access (RDA), Part 3: IRDS Specialization, Ottawa
SC21 N 7199	Remote Database Access (RDA)
SC21 N 7202	Progression of Work on RDA Suspend/Resume and Dialogue Recovery, ISO/IEC JTC1/SC21/WG3 Meeting, Ottawa

Q. DATA MANAGEMENT CONCEPTS:

DIS 7826-1	Representation of Data Elements, Part 1, November 1993
DIS 7826-2	Representation of Data Elements, Part 2, November 1993
ISO/TR 9007	Concepts and Terminology for the Conceptual Schema and the Information Base
ISO/IEC 10032◆	Reference Model of Data Management
CD 11179-1	Coordination of Data Elements, Part 1, Novem ber 1993
CD 11179-2	Coordination of Data Elements, Part 2, November 1993
DIS 11179-3	Coordination of Data Elements, Part 3, Novem ber 1993 (balloting ended February 1994)
DIS 11179-4	Coordination of Data Elements, Part 4, Janaury 1994
CD 11179-5.2	Coordination of Data Elements, Part 5, Janaury 1994
CD 11179-6	Coordination of Data Elements, Part 6, Novem ber 1993
NIST	Database Management Standards: Status and Applicability
SC21 N 197	Concepts and Terminology for the Conceptual Schema and the Information Base, TC97/SC5
SC21 N 236	Assessment Guidelines for Conceptual Schema Language Proposals, TC97/SC21/WG5-3
SC21 N 5137	Data Management Export/Import for SQL and IRDS (to become a three-part standard: Framework; Facilities; Facilities for IRDS)
SC21 N 6614	SC21 Recommended Action to Address Problems of Data Modelling Standards Coordination
SC21 N 6653	Various Contributions to the ISO/IEC JTC1/SC21 Special Group Meeting on Conceptual Schema and Common Data Modelling Facilities
SC21 N 6728	Summary of Planned Contributions to the Renesse Special Meeting on Conceptual Schema Facilities and Common Data Modelling Facilities
SC21 N 6801	Comments on SC21 Recommended Action to Address Problems of Data Modelling Standards Coordination
SC21 N 6929	JTC1 National Body Comments Received on JTC1 N 1756, "Request for Review and Comment on the SC21 Recommended Action to Address Problems of Data Modelling Standards Coordination"
SC21 N 6945	Recommendations and Proposed Work on Conceptual Schema and Data Modelling Facilities
SC21 N 6951	Reference Material on Conceptual Schema and Common Data Modelling Facilities
SC21 N 6952	Report of the 9-13 March 1992 Renesse Meeting of the SC21 Special Group on Conceptual Schema and Common Data Modelling Facilities
SC21 N 6955	Stocktaking of Standards and Standards Projects Which Make Use of a Data Modelling Facility or of a Conceptual Schema
SC21 N 7208	Proposal for an SC21 SWG on Modelling Facilities
SC21 N 7392	US Contribution to the SC21 Special Working Group Meeting on Modelling Facilities, 7-11 December 1992 in Namur, Belgium
SC21 N 8060	Conceptual Schema Modeling Facility
SC21 N 8211	Draft Answer to Question Q3/007, "Support for Distributed Database Systems"
SC21 N 8109	Proposed New Question Q3/011, "Harmonization of Client/Server Capabilities"
SC21/WG3 N 1349	Liaison Report June 1991-May 1992, JTC1/SC7 Software Engineering
SC21/WG3 N 1371	Discussion between JTC1 SC21/WG3 and ISO TC 184/SC5/WG4
SC21/WG3 N 1653	RMDM, SQL92 and SQL3 Mapping Final Reports—Summary and Conclusions, Final V1.1, Inkron Inc., August 1993
SC21/WG3 N 1655	Liaison Statement to CSMF RG, December 1993
SC21/WG3 N 1660	Applicability of the ISO Reference Model of Data Management (ISO 10032:1993) to Client Server Computing, Dr. T. William Olle, October 1993

R. DATABASE LANGUAGES AND CONCEPTS:

ISO 8907	Database Languages - NDL
ISO 9075:1988	Database Language SQL
ISO 9075:1992	Database Languages - SQL (known as SQL2 or SQL-92)
	Cor 1 — Technical Corrigendum 1, January 1994
WD 9075-x	Database Languages - SQL, Part x: SQL Call Level Interface (CLI)
WD 9075-y	Database Languages - SQL, Part y: Persistent SQL Modules
WD 9075.3	Database Languages - SQL3
CD 12227	SQL Ada Module Description Language (SAMeDL)
SC21 N 6737	Object Oriented Task Group Final Report
SC21 N 6759	Recommendation on SQL2 Progression (ISO/IEC DIS 9075)
SC21 N 6760	Minutes of the SQL2 Editing Meeting, Kawagoe
SC21 N 6892	Liaison Statement to SC21/WG4 on Atomic Transaction Interfaces
SC21 N 6931	Working Draft for SQL-3, Interim Database Languages Meeting, Japan
SC21 N 7179	SQL Multimedia and Application Packages
SC21 N 7180	Proposed Draft Answer to Question Q3/001 - Object Database
SC21 N 7183	Liaison Statement to EWOS/EG DBE on Profiling SQL/RDA
SC21 N 7185	Liaison Statement to JTC1/SC14 on Data Elements
SC21 N 7186	Liaison Statement to SC18 on Full-Text Manipulation
SC21 N 8205	SQL Multimedia and Hypermedia Application Packages (SQL/MM) Project Plan (Revised), SC21/WG3, September 1993
SC21/WG3 N 1298	New Project Proposal: SQL ADT Packages
SC21/WG3 N 1345	Letter to Bruce Catley Convenor, JTC1/SC21/WG3, Government Telecommunications Agency/VPD, Ottawa Canada, EWOS, on the European Workshop for Open Systems, Expert Group on Database Enquiry
SC21/WG3 N 1430	DBL Status Report
SC21/WG3 N 1647	ISO SQL Multimedia and Application Packages (SQL/MM), Part 1: Framework, Working Draft
SC21/WG3 N 1613	ISO SQL Multimedia and Application Packages (SQL/MM), Part 2: Full-Text, Working Draft
SC21/WG3 N 1614	ISO SQL Multimedia and Application Packages (SQL/MM), Part 3: Spatial, Working Draft

S. DISTRIBUTED TRANSACTION PROCESSING (TP):

ISO/IEC 10026-1◆	Distributed Transaction Processing (TP), Part 1: Model (X.860:1992)
	PDAM 1 — Amendment 1: Commitment Optimizations
	WDAMs — Draft Amendments to Parts 1-3: Distributed Transaction Processing Dialogue Recovery and User Suspension of a Dialogue
	WDAMs — Draft Amendments to Parts 1-3: Transaction Processing Association Pool Management
	WDAMs — Draft Amendments to Parts 1-3: Transaction Processing Sub-Transactions
	WDAMs — Draft Amendments to Parts 1-3: Transaction Processing Separate Data and Commit Associations
	WDAMs — Draft Amendments to Parts 1-3: Transaction Processing Security
ISO/IEC 10026-2◆	Distributed Transaction Processing (TP), Part 2: Service (X.861:1992)
	PDAM 1 — Amendment 1: Commitment Optimizations,
ISO/IEC 10026-3◆	Distributed Transaction Processing (TP), Part 3: Transaction Processing Protocol Specification (X.862)
	PDAM 1 — Amendment 1: Commitment Optimizations,
ISO/IEC 10026-4	Distributed Transaction Processing (TP), Part 4: PICS Proforma
ISO/IEC 10026-5	Distributed Transaction Processing (TP), Part 5: Application Context Proforma
ISO/IEC 10026-6	Distributed Transaction Processing (TP), Part 6: Unstructured Data Transfer
CD 10026-7	Distributed Transaction Processing (TP), Part 7: Message Queueing
WD 10026-x	Distributed Transaction Processing (TP), Part x: Dialogue Recovery
WD 10026-y	Distributed Transaction Processing (TP), Part y: TP Association Pool Management Function
CD 11587.2	Application Context for Systems Management with Transaction Processing
DISP 12061-1	ISPs ATP nn - OSI Distributed Transaction Processing, Part 1: Introduction, 1993
DISP 12061-2	ISPs ATP nn - OSI Distributed Transaction Processing, Part 2: Support of the OSI TP APDUs, 1993
DISP 12061-3	ISPs ATP nn - OSI Distributed Transaction Processing, Part 3: Support of the CCR Protocols, 1993
DISP 12061-4	ISPs ATP nn - OSI Distributed Transaction Processing, Part 4: Support of ACSE, Presentation and Session Protocols, 1993
DISP 12061-5	ISPs ATP nn - OSI Distributed Transaction Processing, Part 5: ATP 11, Application Supported Transactions with Polarized Control, 1993

DISP 12061-6	ISPs ATP an - OSI Distributed Transaction Processing, Part 6: ATP 12, Application Supported Transactions with Shared Control, 1993
DISP 12061-7	ISPs ATP an - OSI Distributed Transaction Processing, Part 7: ATP 21, Provider Supported Transactions in Unchained Mode with Polarized Control, 1993
DISP 12061-8	ISPs ATP an - OSI Distributed Transaction Processing, Part 8: ATP 22, Provider Supported Transactions in Unchained Mode with Shared Control, 1993
pDISP 12061-9	ISPs ATP an - OSI Distributed Transaction Processing, Part 9: ATP 31, Provider Supported Transactions in Chained Mode with Polarized Control, 1993
pDISP 12061-10	ISPs ATP an - OSI Distributed Transaction Processing, Part 10: ATP 32, Provider Supported Transactions in Chained Mode with Shared Control, 1993
pDISP 12061-11	ISPs ATP an - OSI Distributed Transaction Processing, Part 11: TP Transaction Recovery Application Context, 1993
pDISP 12061-x	ISPs ATP an - OSI Distributed Transaction Processing, Part x: Systems Profiling for TP, 1993
pDISP 12061-y	ISPs ATP an - OSI Distributed Transaction Processing, Part y: Development of PTS for TP, 1993
SC21 N 6756	TP/CCR One-Phase Commitment
SC21 N 7156	Proposed NP for Transaction Processing Abstract Test Suites
SC21 N 7165	TP Commitment Optimization Issues and Resolutions
SC21 N 7166	Requirements and Issues for the Separation of Data and Commitment Flows in OSI TP
SC21 N 7167	Request for Contributions on OSI TP Subtransactions
SC21 N 7168	Request for Comments on Issues Concerning TP Association Pool Management
SC21 N 7171	Revised TP Test Suite Structure and Test Purposes
SC21 N 7172	General Principles for the Development of TP Test Cases
SC21 N 7173	Open Issues and Questions for the Development of TP Test Cases
SC21 N 7175	Liaison Statement to SC6 on Requirement for Non-Blocking Transport Expedited Service
SC21 N 7417	Association Management Concepts
SC21 N 7625	Status of Work on the Separation of Data and Commit Flows in OSI-TP
SC21 N 7626	Request for Contributions for OSI-TP Subtransactions
SC21 N 7644	TP Commitment Optimizations - Topics and Their Resolution
SC21 N 7672	Revised Working Draft for TP Test Suite Structure
SC21 N 7676	Initial Abstract Test Suite for TP
SC21 N 8151	Status of Work on the Subtransactions in OSI TP, SC21/WG8, July 1993
SC21 N 8152	Status of Work on the Separation of Data and Commit Flows in OSI TP, SC21/WG8, July 1993
SC21 N 8216	Conformance Test Suite for TP Protocol, Part 1: Test Suite Structure and Test Purposes
SC21 N 8321	Requirement for Partial Rollback, USA, November 1993
SC21 N 8322	Response to SC21 N 8067 on TP with RPC, USA, November 1993
SC21/WG1 N 1253	Use of Quality of Services in ODP Trader
SC21/WG5 N 673	Minutes of the TP Group Meeting, Ottawa, 21-29 May 1992
ITU-TS X.860	Distributed Transaction Perocessing: Model (ISO 10026-1), 1992
ITU-TS X.861	Distributed Transaction Perocessing: Service (ISO 10026-2), 1992
ITU-TS X.862	Distributed Transaction Perocessing: Protocol Specification (ISO 10026-3), Draft, 1993
ITU-TS X.863	Information Technology - Open Systems Interconnection - Distributed Transaction Perocessing: PICS Proforma (ISO 10026-4), Draft, 1993

T. OPEN DISTRIBUTED PROCESSING (ODP):

WD 10746-1	Basic Reference Model for Open Distributed Processing, Part 1: Overview and Guide to Use (merged with old 10756-4) (X.901)
CD 10746-2.3	Basic Reference Model for Open Distributed Processing, Part 2: Descriptive Model (X.902)
CD 10746-3.2	Basic Reference Model for Open Distributed Processing, Part 3: Descriptive Model (X.903)
WD 10746-4	Basic Reference Model for Open Distributed Processing, Part 4: Architectural Semantics, Specification Techniques, and Formalisms (formerly User Model) (X.904)
SC21 N 6972	Draft Answer to Q6/2 - Relationship Between the OSI Upper Layer Architecture and ODP
SC21 N 7042	The RM-ODP and Standardization of APIs
SC21 N 7051	Proposed Draft Answer to Question Q7/1 on the Suitability of the Formal Description Z for Use in ODP
SC21 N 7052	Editing Instructions for a Technical Report on Use of FDTs in ODP
SC21 N 7057	List of Open and Resolved Issues
SC21 N 7088	Proposed New Question Q1/66 on ODP Conformance Testing Methodology
SC21 N 7425	Draft First Report on the New Work Area on Programmatic Interfaces
SC21 N 8285	Position on the ODP Standards Process and Cooperation with de facto Standards Organizations, AFNOR, October 1993
SC21 N 8409	Information Technology - Open Systems Interconnection - ODP Trading Function, January 1994
SC21/WG7 N 783	An Integrated Approach to Trader Contexts, August 1993
SC21/WG7 N 811	Relations of Formal Descriptions of Different ODP Viewpoint Models, August 1993

SC21/WG7 N 821	Discussion Note on RM-ODP Part 4, August 1993
SC21/WG7 N 823	Joint Action Plan SC21/WG7 and WG7-ITU-TS/Q16/7 (ITU-TS Format), August 1993
SC21/WG7 N 836	Liaison Contributions for SC21/WG7, SC21/WG3, August 1993
SC21/WG7 N 852	Outline of Information Specification for ODP Trader, Australia, October 1993
SC21/WG7 N 862	An ODP Architectural Semantics in Z, UK, October 1993
SC21/WG7 N 863	An ODP Architectural Semantics in LOTOS, UK, October 1993
ITU-TS X.901	Basic Reference Model for Open Distributed Processing: Overview and Guide to Use (ISO 10746-1), Draft, 1993
ITU-TS X.902	Basic Reference Model for Open Distributed Processing: Descriptive Model (ISO 10746-2), Draft, 1993
ITU-TS X.903	Basic Reference Model for Open Distributed Processing: Prescriptive Model (ISO 10746-3), Draft, 1993
ITU-TS X.904	Basic Reference Model for Open Distributed Processing: Architectural Semantics (ISO 10746-4), Draft, 1993
ITU-TS X.tr	Basic Reference Model for Open Distributed Processing: Use of Formal Description Technique for ODP, Draft, 1993
ITU-TS X.trader	Basic Reference Model for Open Distributed Processing: ODP Trader, Draft, 1993

U. GRAPHICAL KERNEL SYSTEM (GKS):

ISO 7942	Graphical Kernel System (GKS) Functional Description	
	AM 1	Audit Trail Metafile
ISO 8651-1	GKS Language Bindings, Part 1: FORTRAN	
ISO 8651-2	GKS Language Bindings, Part 2: Pascal	
ISO 8651-3	GKS Language Bindings, Part 3: Ada	
ISO/IEC 8651-4	GKS Language Bindings, Part 4: C	
ISO 8805	GKS for Three Dimensions (GKS-3D) Functional Description	
	WDAM 1	Name Set Addendum
DIS 8806-1	GKS-3D Language Bindings, Part 1: FORTRAN	
DIS 8806-3	GKS-3D Language Bindings, Part 3: Ada	
ISO/IEC 8806-4	GKS-3D Language Bindings, Part 4: C	

V. PROGRAMMER'S HIERARCHICAL INTERACTIVE GRAPHICS SYSTEM (PHIGS):

ISO 9592-1	Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings, Part 1: Functional Description	
	AM 1	PHIGS Plus Support
ISO 9592-2	PHIGS Language Bindings, Part 2: Archive File Format	
	AM 1	PHIGS Plus Support
ISO 9592-3	PHIGS Language Bindings, Part 3: Clear-Text Encoding of Archive File	
	AM 1	Incorporation of PHIGS Plus
ISO 9592-4	PHIGS Language Bindings, Part 4: PHIGS Plus [SC24 N 224]	
ISO/IEC 9593-1	PHIGS Language Bindings, Part 1: FORTRAN	
DIS 9593-2	PHIGS Language Bindings, Part 2: Extended Pascal	
ISO 9593-3	PHIGS Language Bindings, Part 3: Ada	
ISO 9593-4	PHIGS Language Bindings, Part 4: C	

W. DIALOGUES WITH GRAPHICAL DEVICES:

ISO 9636-1	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 1: Overview, Profiles, and Conformance
ISO 9636-2	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 2: Control, Negotiation, and Errors
ISO 9636-3	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 3: Output and Attributes
ISO 9636-4	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 4: Segmentation
ISO 9636-5	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 5: Input and Echoing
ISO 9636-6	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 6: Raster
WD 9636-8	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 8: FORTRAN Language Binding of CGI

WD 9636-11	Computer Graphics - Interfacing (CGI) Techniques for Dialogues with Graphical Devices - Functional Specification, Part 11: C Language Binding of CGI
DIS 9637-1	Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 1: Character Encoding
ISO/IEC 9637-2	Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 2: Binary Encoding
DIS 9637-3	Interface Techniques for Dialogues with Graphical Devices -- CGI Data Stream Encoding -- Part 3: Clear Text Encoding
DIS 9638-1	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings, Part 1: FORTRAN
DIS 9638-2	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings, Part 2: Pascal
DIS 9638-3	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings, Part 3: Ada
DIS 9638-4	Interface Techniques for Dialogues with Graphical Devices -- CGI Language Bindings, Part 4: C
DIS 10641	Conformance Testing of Implementations of Graphics Standards

X. DOCUMENT EXCHANGE--ODA, ODIF, DOAM, DFR, AND DTAM:

ISO 8211	Specification for a Data Descriptive File for Information Interchange	
DIS 8211.2	Specification for a Data Descriptive File for Information Interchange, Edition 2	
ISO 8613-1•	Office Document Architecture (ODA) and Interchange Format, Part 1: Introduction and General Principles	
	AM 1	Document Application Profile Proforma and Notation
	AM 2	Conformance Testing Methodology
ISO 8613-2•	ODA and Interchange Format, Part 2: Document Structures	
	PDAD 1	Formal Specification of ODA Document Structures
DIS 8613-3	ODA and Interchange Format, Part 3: Abstract Interface for Manipulation of ODA Documents	
ISO 8613-4•	ODA and Interchange Format, Part 4: Document Profile	
ISO 8613-5•	ODA and Interchange Format, Part 5: Office Document Interchange Format (ODIF)	
ISO 8613-6•	ODA and Interchange Format, Part 6: Character Content Architectures	
ISO 8613-7•	ODA and Interchange Format, Part 7: Raster Graphics Content Architectures	
ISO 8613-8•	ODA and Interchange Format, Part 8: Geometric Graphics Content Architectures	
	DAD 1	Tiled Raster Graphics
	DAM 2.2	Color
	DAD 3	Alternative Representation
	DAD 4	Security
	DAM 5.2	Streams
	DAD 6	Styles
	PDAM 10	ODA External References and Document Fragments
CD 8613-9	ODA and Interchange Format, Part 9: Audio Content Architecture	
ISO 8613-10	ODA and Interchange Format, Part 10: Formal Specifications	
	AM 1	Formal Specification of the Document Profile
	AM 2	Formal Specification of the Raster Graphics Content Architectures
	AM 3	Formal Specification of ODA Character Content Architectures
	AM 4	Formal Specification of ODA Geometric Graphics Content Architectures
	AM 5	Formal Specification of the Defaulting Mechanism for Defaultable Attributes
CD 8613-11	ODA Spreadsheet	
DIS 8613-12	ODA Identification of Document Fragments	
ISO/IEC 10031-1	Distributed Office Applications Model (DOAM), Part 1: General Model	
ISO/IEC 10031-2	Distributed Office Applications Model (DOAM), Part 2: Referenced Data	
ISO/IEC 10166-1	Document Filing and Retrieval (DFR), Part 1: Abstract Service Definition and Procedures	
ISO/IEC 10166-2	Document Filing and Retrieval (DFR), Part 2: Protocol Specification	
ISO/IEC TR 10183	ODA and Interchange Format - Testing Methodology and Abstract Cases - Implementation Testing	
CD 10303-11	Standard for Exchange of Product Model Data (STEP), Part 11: EXPRESS	
pDISP 12064-1	International Standardized Profiles FOD nnn - ODA - Open Document Format: Image Applications - Simple Document Structure - Raster Graphics Content Architecture, Part 1: FOD 112, Document Applications Profile, August 1993 (balloting ended December 1993)	
SC21 N 6227	Virtual Terminal Support of ODA	
SC21 N 6667	Contributions from ISO/IEC JTC1/SC18 Regarding the Progression of Work on Multimedia and Hypermedia Model/Framework	
SC21 N 7430	Working Draft of the Technical Report on Multimedia and Hypermedia: Model and Framework	
SC21 N 8256	Disposition of Comments Report and Final Work Item Definition for "Engagement Scheduling and Recording Application within the Distributed Office Applications Model (DOAM)," October 1993	

SC24 N 847	Initial Draft PREMO (Presentation Environment for Multimedia Objects).
ITU-TS T.400	Introduction to Document Architecture, Transfer and Manipulation
ITU-TS T.410/S	First Extension (January 1991) to the T.410 Series (1988) of Recommendations Contained in the CCITT Blue Book, Fascicle VII.6
ITU-TS T.411	Open Document Architecture (ODA) and Interchange Format - Introduction and General Principles (see ISO 8613-1)
ITU-TS T.411/F	Annex F to Recommendation T.411
ITU-TS T.412	Open Document Architecture (ODA) and Interchange Format - Document Structures (see ISO 8613-2)
ITU-TS T.414	Open Document Architecture (ODA) and Interchange Format - Document Profile (see ISO 8613-4)
ITU-TS T.415	Open Document Architecture (ODA) and Interchange Format - Open Document Interchange Format (ODIF) (see ISO 8613-5)
ITU-TS T.416	Open Document Architecture (ODA) and Interchange Format - Character Content Architectures (see ISO 8613-6)
ITU-TS T.417	Open Document Architecture (ODA) and Interchange Format - Raster Graphics Content Architectures (see ISO 8613-7)
ITU-TS T.418	Open Document Architecture (ODA) and Interchange Format - Geometric Graphics Content Architectures (see ISO 8613-8)
ITU-TS T.419	Document Transfer and Manipulation (DTAM) - Composite Graphics Content Architectures
ITU-TS T.431	Document Transfer and Manipulation (DTAM) - Services and Protocols, Introduction and General Principles
ITU-TS T.432	Document Transfer and Manipulation (DTAM) - Services and Protocols, Service Definition
ITU-TS T.433	Document Transfer and Manipulation (DTAM) - Services and Protocols, Protocol Specification
ITU-TS T.441	Document Transfer and Manipulation (DTAM) - Operational Structure
ITU-TS T.501 Rev 1	Document Application Profile MM for the Interchange of Formatted Mixed Mode Documents (Mixed Mode)
ITU-TS T.502 Rev 1	Document Application Profile PM-11 for the Interchange of Processable Form Documents (Teletex Processable Mode)
ITU-TS T.503	Document Application Profile for the Interchange of Group 4 Facsimile Documents
ITU-TS T.504 Rev 1	Document Application Profile for Videotex Interworking
ITU-TS T.505	Document Application Profile PM-26 for the Interchange of Mixed Content Documents in Processable and Format Forms
ITU-TS T.521	Communication Application Profile BT0 for Document Bulk Transfer Based on the Session Service (According to Rules Defined in T.62 bis)
ITU-TS T.522	Communication Application Profile BT1 for Document Bulk Transfer
ITU-TS T.523 Rev 1	Communication Application Profile DM-1 for Videotex Interworking
ITU-TS T.541 Rev 1	Operational Application Profile for Videotex Interworking
ITU-TS T.561	Terminal Characteristics for Mixed Mode of Operation MM
ITU-TS T.562	Terminal Characteristics for Teletex Processing Mode PM1
ITU-TS T.563 Rev 1	Terminal Characteristics for Group 4 Facsimile Apparatus
ITU-TS T.564 Rev 1	Gateway Characteristics for Videotex Interworking

Y. PICTURE DESCRIPTION INFORMATION EXCHANGE:

ISO 8632-1	Computer Graphics Metafile (CGM): Metafile for the Storage and Transfer of Picture Description Information, Part 1: Functional Specification AM 1 — Audit Trail Metafile PDAD 2 — 3D Static Picture Capture Metafile DAM 3 — Part 1: Functional Specification DAM 4 — Rules for Profiles
ISO 8632-2	CGM: Metafile for the Storage and Transfer of Picture Description Information, Part 2: Character Encoding AM 1 and DAM 3
ISO 8632-3	CGM: Metafile for the Storage and Transfer of Picture Description Information, Part 3: Binary Encoding AM 1 and DAM 3
ISO 8632-4	CGM: Metafile for the Storage and Transfer of Picture Description Information, Part 4: Clear Text Encoding
ISO 9281-1	Identification of Picture Coding Methods, Part 1: Identification, 1990
ISO 9281-2	Identification of Picture Coding Methods, Part 2: Procedure for Registration, 1990
ISO 9282-1	Coded Representation of Computer Graphics Images, Part 1: Encoding Principles for Picture Representation in a 7-bit or 8-bit Environment, 1988
ISO 9282-2	Coded Representation of Computer Graphics Images, Part 2: Incremental Encoding of Point Lists in a 7-bit or 8-bit Environment, 1992
CD 10743	Standard Music Description Language (SMDL)

ISO/IEC 10918-1	Digital Compression and Coding of Continuous-Tone Still Images, Part 1: Requirements and Guidelines, 1993
DIS 10918-2	Digital Compression and Coding of Continuous-Tone Still Images, Part 2: Compliance Testing
WD 10918-3	Digital Compression and Coding of Continuous-tone Still Images, Part 3: Extensions
ISO/IEC 11072	Computer Graphics - Reference Model of Computer Graphics
ISO/IEC 11172-1	Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 1: Systems, 1993
ISO/IEC 11172-2	Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 2: Video, 1993
ISO/IEC 11172-3	Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 3: Audio, 1993
CD 11172-4	Coding of Moving Pictures and Associated Audio for Digital Storage Media Up to About 1,5 Mbit/s, Part 4: Conformance Testing, 1993
WD 11172-5	Coding of Moving Pictures and Associated Audio for Digital Storage Media Up to About 1,5 Mbit/s, Part 5: Technical Report on Software for ISO/IEC 11172, 1993
ISO/IEC 11544	Coded Representation of Bi-level and Limited Bits-per-pixel Still Pictures, 1993
ISO/IEC 11558	Data Compression for Information Interchange, Adaptive Coding with Embedded Dictionary, DCLZ Algorithm
DIS 12087-1	Image Processing and Interchange (IPI) Standard, Part 1, Common Architecture for Imaging (CAI)
DIS 12087-2	Image Processing and Interchange (IPI) Standard, Part 2, Programmer's Imaging Kernel System (PIKS)
DIS 12087-3	Image Processing and Interchange (IPI) Standard, Part 3, Image Interchange Facility (IIF)
CD 13522-1	Coding of Multimedia and Hypermedia Information, Part 1: MHEG Objects Representation - Base Notation (ASN.1), 1993
WD 13522-2	Coding of Multimedia and Hypermedia Information, Part 2: Alternate Notation (SMSL), 1993
WD 13522-3	Coding of Multimedia and Hypermedia Information, Part 3: MHEG Extensions for Scripting Language Support, 1993
CD 13818-1	Generic Coding of Moving Pictures and Associated Audio Information, Part 1: Systems, SC29/WG11, November 1993 [SC29 N 634] (DIS expected March 1994, IS in November 1994]
CD 13818-2	Generic Coding of Moving Pictures and Associated Audio Information, Part 2: Video, SC29/WG11, November 1993 [SC29 N 634] (DIS expected March 1994, IS in November 1994]
CD 13818-3	Generic Coding of Moving Pictures and Associated Audio Information, Part 3: Audio, SC29/WG11, November 1993 [SC29 N 635] (DIS expected March 1994, IS in November 1994]
WD 13818-4	Generic Coding of Moving Pictures and Associated Audio Information, Part 4: Conformance Testing, SC29/WG11, November 1993 [SC29 N 636] (CD expected November 1994, DIS in March 1995, IS in November 1995]
WD 13818-5	Generic Coding of Moving Pictures and Associated Audio Information, Part 5: Technical Report on Software for ISO/IEC 13818, SC29/WG11 (WD expected July 1994, CD in November 1994, DIS in March 1995, IS in November 1995]
WD 13818-6	Generic Coding of Moving Pictures and Associated Audio Information, Part 6: System Extensions, SC29/WG11 (WD expected November 1994, CD in March 1995, DIS in November 1995, IS in July 1996]
WD 13818-7	Generic Coding of Moving Pictures and Associated Audio Information, Part 7: Audio Extensions, SC29/WG11 (WD expected November 1996, CD in March 1997, DIS in July 1997, IS in March 1998]
SC21 N 5165	FTAM Constraint Set and Document Types for CGM
SC21 N 6916	Liaison Statement to SC21/WG6 Concerning the Use of ASN.1 in the Image Processing and Interchange Image Interchange Facility (IPI-IIF) Standard
SC21 N 6983	Liaison Statement to SC24 Concerning the Use of ASN.1 in the IPI/IIF Standards
SC29 N 363	Image Compression Across Multiple Components
SC29 N 364	Lossy/Lossless Coding of Bi-level Images
SC29 N 365	Compression of Up to 5-D Images
SC29 N 366	Lossless Compression of Continuous-Tone Still Pictures
SC29 N 367	Very-low Bitrate Audio-Visual Coding (four parts: Systems, Video, Audio, and Conformance Testing), 1993
SC29 N 368	Low-Bit-Rate Audio Coding, 1993
ITU-TS T.82	Coded Representation of Picture and Audio Information-Progressive Bi-level Image Compression

Z. STANDARD GENERALIZED MARKUP LANGUAGE (SGML):

ISO 8879	Standard Generalized Markup Language (SGML) AM 1 Amendment 1
ISO 9069	SGML Support Facilities - SGML Document Interchange Format (SDIF)
ISO/IEC 9070	SGML Support Facilities - Registration Procedures for Public Text Owner Identifiers
WDTR 9573-1	SGML Support Facilities - Techniques for Using SGML, Part 1: SGML Tutorial

WDTR 9573-2	SGML Support Facilities - Techniques for Using SGML, Part 2: Basic Technique
WDTR 9573-3	SGML Support Facilities - Techniques for Using SGML, Part 3: Advanced Techniques - Using LINK and CONCUR
WDTR 9573-4	SGML Support Facilities - Techniques for Using SGML, Part 4: Advanced Techniques - Using SHORTREF to Indicate Markup
WDTR 9573-5	SGML Support Facilities - Techniques for Using SGML, Part 5: Using Non-Latin Alphabets
WDTR 9573-6	SGML Support Facilities - Techniques for Using SGML, Part 6: Referencing and Synchronization
WDTR 9573-7	SGML Support Facilities - Techniques for Using SGML, Part 7: Mathematics and Chemistry
WDTR 9573-8	SGML Support Facilities - Techniques for Using SGML, Part 8: Tables
WDTR 9573-9	SGML Support Facilities - Techniques for Using SGML, Part 9: Using SGML for Computer to Computer Interchange
WDTR 9573-10	SGML Support Facilities - Techniques for Using SGML, Part 10: Designing Applications for Database Interfacing
ISO/IEC TR 9573-11	SGML Support Facilities - Techniques for Using SGML, Part 11: Application at ISO Central Secretariat for International Standards and Technical Reports to TR status
ISO/IEC TR 9573-12	SGML Support Facilities - Techniques for Using SGML, Part 12: Public Entity Sets for General and Publishing Symbols
ISO/IEC TR 9573-13	SGML Support Facilities - Techniques for Using SGML, Part 13: Public Entity Sets for Mathematics and Sciences
WDTR 9573-14	SGML Support Facilities - Techniques for Using SGML, Part 14: Public Entity Sets for Latin Based Alphabets
WDTR 9573-15	SGML Support Facilities - Techniques for Using SGML, Part 15: Public Entity Sets for Non-Latin Based Alphabets
WDTR 9573-16	SGML Support Facilities - Techniques for Using SGML, Part 16: Public Entity Sets for Ideograms
ISO/IEC TR 10037	SGML and Text-Entry Systems - Guidelines for SGML Syntax-Directed Editing Systems
ISO/IEC 10179	Document Style Semantics and Specification Language (DSSSL)
DIS 10180	Standard Page Description Language (SPDL)
ISO/IEC 10744	Hypermedia/Time-based Structuring Language (HyTime)

AA. OTHER APPLICATION LAYER STANDARDS:

DP 9955	Methodology and Guidelines for the Development of Application Protocols for Banking Information Interchange
DIS 10161-2	Information and Documentation - Open Systems Interconnection - Interlibrary Loan Application Protocol Specification, Part 2: Protocol Implementation Conformance Statement Proforma
pDISP 12065-1	International Standardized Profiles ALD 1n - Library and Documentation - Search and Retrieve, Part 1: Specification of ACSE, Presentation, and Session Protocols for Use by Library and Documentation, August 1993
pDISP 12066-1	International Standardized Profiles ALD 2n - Library and Documentation - Interlibrary Loan, Part 1: Generic, August 1993
pDISP 12066-2	International Standardized Profiles ALD 2n - Library and Documentation - Interlibrary Loan, Part 2: Using Connection-Oriented ACSE, August 1993

(This page intentionally left blank)

IX. MISCELLANEOUS STANDARDS[27]

- A. Integrated Services Digital Network (ISDN): General Standards
- B. Electronic Data Interchange (EDI)
- C. Telematic Services
- D. Vocabulary and Representations
- E. Coded Character Sets
- F. Man-Machine Language (MML)
- G. Software Development and Documentation
- H. Information Processing Equipment

A. INTEGRATED SERVICES DIGITAL NETWORK (ISDN): GENERAL STANDARDS[28]

ISO/IEC 9574◆	Provision of the OSI Connection-Mode Network Service by Packet Mode Terminal Equipment Connected to an ISDN
ITU-TS I.110	General Structure of the I-Series Recommendations
ITU-TS I.111	Relationship with Other Recommendations Relevant to ISDNs
ITU-TS I.112 Rev 1	Vocabulary of Terms for ISDNs
ITU-TS I.113	Vocabulary of Terms for Broadband Aspects of ISDNs
ITU-TS I.114	Vocabulary of Terms for Universal Personal Telecommunication
ITU-TS I.120	Integrated Service Digital Networks (ISDNs)
ITU-TS I.121	Broadband Aspects of ISDNs
ITU-TS I.122 Rev 1	Framework for Providing Additional Packet Mode Bearer Services
ITU-TS I.144	Number Identification Supplementary Services
ITU-TS I.150 Rev 1	B-ISDN Asynchronous Transfer Mode Functional Characteristics
ITU-TS I.200	Guidance to the I.200 Series of Recommendations
ITU-TS I.210 Rev 1◆	Principles of Telecommunications Services Supported by an ISDN
ITU-TS I.211 Rev 1◆	B-ISDN Service Aspects
ITU-TS I.212◆	Teleservices Supported by an ISDN
ITU-TS I.220	Common Dynamic Description of Basic Telecommunication Services
ITU-TS I.221 Rev 1	Common Specific Characteristics of Services
ITU-TS I.223.1	ISDN Frame Mode Bearer services (FMBS) - ISDN Frame Relaying Bearer Services
ITU-TS I.223.2	ISDN Frame Mode Bearer services (FMBS) - ISDN Frame Switching Bearer Service
ITU-TS I.230	Definition of Bearer Service Categories
ITU-TS I.231◆	Circuit-Mode Bearer Service Categories
ITU-TS I.231.9◆	Circuit mode 64 kbit/s 8 kHz structured multi-use bearer service category
ITU-TS I.232◆	Packet Mode Bearer Service Categories
ITU-TS I.240◆	Definition of Teleservices
ITU-TS I.241◆	Teleservices Supported by an ISDN
ITU-TS I.241.7◆	Telephony 7 kHz
ITU-TS I.250◆	Definition of Supplementary Services
ITU-TS I.251	Number Identification Supplementary Services
ITU-TS I.252	Call Offering Supplementary Services
ITU-TS I.253	Call Completion Supplementary Services
ITU-TS I.253.1	Call Waiting (CW) Supplementary Service
ITU-TS I.254	Multiparty Supplementary Services
ITU-TS I.255	Community of Interest Supplementary Services
ITU-TS I.255.3	Multi-level Precedence and Preemption Service (MLPP) - Description Preference Service
ITU-TS I.255.4	Priority Service
ITU-TS I.256	Changing Supplementary Services
ITU-TS I.256.2a	Advice of Charge: Charging Information at Call Set-Up Time
ITU-TS I.256.2b	Advice of Charge: Charging Information During Call
ITU-TS I.256.2c	Advice of Charge: Charging Information at End of the Call

27 The symbol ◆ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy*.

28 A list of ITU-TS (formerly CCITT) 1992 Recommendations on ISDN is provided in Appendix E, Section II.B.

ITU-TS I.257	Additional Information Transfer Supplementary Services
ITU-TS I.320	ISDN Protocol Reference Model
ITU-TS I.321	B-ISDN Protocol Reference Model and Its Application
ITU-TS I.325 Rev 1	Reference Configurations for ISDN Connection Types
ITU-TS I.327 Rev 1	B-ISDN Functional Architecture
ITU-TS I.333 Rev 1	Terminal Selection in ISDN
ITU-TS I.340	ISDN Connection Types
ITU-TS I.410	General Aspects and Principles Relating to Recommendations on ISDN User-Network Interfaces
ITU-TS I.411 Rev 1	ISDN User-Network Interfaces - Reference Configurations
ITU-TS I.412	ISDN User-Network Interfaces - Interface Structures and Access Capabilities
ITU-TS I.413 Rev 1	B-ISDN User Network Interface
ITU-TS I.420	Basic User-Network Interface (ISDN)
ITU-TS I.421	Primary Rate User-Network Interface (ISDN)
ITU-TS I.560	Requirements to be Met in Providing the Telex Service Within the ISDN
ITU-TS I.601	General Maintenance Principles of ISDN Subscriber Access and Subscriber Installation
ITU-TS I.602	Application of Maintenance Principles to ISDN Subscriber Installation
ITU-TS I.603	Application of Maintenance Principles to ISDN Basic Accesses
ITU-TS I.604	Application of Maintenance Principles to ISDN Primary Rate Accesses
ITU-TS I.605	Application of Maintenance Principles to Static Multiplexed ISDN Basic Accesses
ITU-TS I.610 Rev 1	DAM Principles of the B-ISDN Access

B. ELECTRONIC DATA INTERCHANGE (EDI):

ISO 9735	Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) - Application Level Syntax Rules AM1 Amendment 1
SC21 N 3885	UN/EDIFACT Information Pack
SC21 N 5635	Report of the Special Working Group on a Conceptual Model for Electronic Data Interchange Standards and Services (SWG-EDI)
SC21 N 6224	Proposed EDIFACT/FTAM Document Type
SC21 N 7184	Liaison Statement to JTC1/WG3 on EDI

C. TELEMATIC SERVICES:

DP 9071-1.2	Text and Office Systems - Basic and Optional Requirements, Part 1: Facsimile Equipment
DP 9071-2.2	Text and Office Systems - Basic and Optional Requirements, Part 2: Text Communications Terminals
ITU-TS F. 30 Rev 1	Use of Various Sequences of Combinations for Special Purposes
ITU-TS F. 63 Rev 1	Additional Facilities in the International Telex Service
ITU-TS F. 69 Rev 1	Plan for Telex Destination Codes
ITU-TS F. 72 Rev 1	International Telex Store and Forward - General Principles and Operational Aspects
ITU-TS F. 140 Rev 1	Point-to-Multipoint Telecommunication Service Via Satellite
ITU-TS F. 160 Rev 1	General Operational Provisions for the International Public Facsimile Services
ITU-TS F. 180 Rev 1	General Operational Provisions for the International Public Facsimile Service Between Subscribers' Stations (Telefax)
ITU-TS F. 182 Rev 1	Operational Provisions for the International Public Facsimile Service Between Subecriber Stations with Group 3 Facsimile Machines (Telefax 3)
ITU-TS F. 184 Rev 1	Operational Provisions for the International Public Facsimile Service Between Subscriber Stations with Group 4 Facsimile Machines (Telefax 4)
ITU-TS F. 200	Teletex Service
ITU-TS F. 200/C	Teletex Service, Annex C: Mixed Mode of Operation
ITU-TS F. 201 Rev 1	Internetworking Between the Teletex Service and the Telex Service
ITU-TS F. 220 Rev 1	Service requirements Unique to the Processable Mode Number One (PM1)
ITU-TS F. 300 Rev 1	Videotext Service
ITU-TS F. 551	Service Recommendation for Telematic File Transfer Within Telefax 3, Telefax 4, Teletex and Message Handling Services
ITU-TS F. 581	Guidelines for Programming Communication Interfaces Definition (Service Recommendation)
ITU-TS F. 600 Rev 1	Service and Operational Principles for Public Data Transmission Services
ITU-TS F. 710	General Principles for Audiographic Conference Services
ITU-TS F. 850	Principles of Universal Personal Telecommunication
ITU-TS F. 901	Usability Evaluation of Telecommunication Services
ITU-TS T. 0	Classification of Facsimile Apparatus for Document Transmission over the Public Networks
ITU-TS T. 4 Rev 3	Standardization of Group 3 Facsimile Apparatus for Document Transmission
ITU-TS T. 5	General Aspects of Group 4 Facsimile Apparatus

ITU-TS T. 6	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus
ITU-TS T. 22	Standardized Test Charts for Document Facsimile Transmissions
ITU-TS T. 30 Rev 3	Procedures for Document Facsimile Transmission in the General Switched Telephone Network
ITU-TS T. 35	Procedure for the Allocation of Defined Codes for Non-Standard Facilities
ITU-TS T. 50	International Alphabet No. 5
ITU-TS T. 51	Coded Character Sets for Telematic Services
ITU-TS T. 52	Non-Latin Coded Character Sets for Telematic Services
ITU-TS T. 60 Rev 1	Terminal Equipment for Use in the Teletex Service
ITU-TS T. 61 Rev 1	Character Repertoire and Coded Character Sets for the International Teletex Service
ITU-TS T. 62 Rev 1	Control Procedures for Teletex and Group 4 Facsimile Services
ITU-TS T. 62 bis Rev 1	Control Procedures for Teletex and Group 4 Facsimile Services Based on Recommendations X.215/X.225
ITU-TS T. 63 Rev 1	Provision for Verification of Teletex Terminal Compliance
ITU-TS T. 64 Rev 1	Conformance testing procedures for the teletex Recommendations
ITU-TS T. 70 Rev 1	Network-Independent Basic Transport Service for the Telematic Services
ITU-TS T. 71	LAPB Extended for Half-Duplex Physical Level Facility
ITU-TS T. 72	Terminal Capabilities for Mixed Mode of Operation
ITU-TS T. 73	Document Interchange Protocol for the Telematic Services
ITU-TS T. 82	Coded Representation of Picture and Audio Information-Progressive Bi-level Image Compression
ITU-TS T. 90	Teletex Requirements for Internetworking with the Telex Service
ITU-TS T. 91	Teletex Requirements for Real-Time Internetworking with the Telex Service in a Packet-Switching Network Environment
ITU-TS T. 101 Rev 1	International Interworking for Videotex Services
ITU-TS T. 102	Protocols for Syntax-Based Videotex Using ISDN Circuit Mode
ITU-TS T. 103	Protocols for Syntax-Based Videotex Using ISDN Packet Mode
ITU-TS T. 104	Packet Mode Access for Syntax-Based Videotex Via PSTN
ITU-TS T. 105	Syntax-Based Videotex Application Layer Protocol
ITU-TS T. 106	Framework for Videotex Terminal Protocols
ITU-TS T. 122	Multipoint Communications Service
ITU-TS T. 123	Protocol Stacks For Audiographic And Audiovisual Teleconference Applications
ITU-TS T. 330	Telematic Access to Interpersonal Messaging System

D. VOCABULARY AND REPRESENTATIONS:

ISO 2382-1	Vocabulary, Part 1: Fundamental Terms
ISO 2382-2	Vocabulary, Part 2: Arithmetic and Logic Operations
ISO 2382-3	Vocabulary, Part 3: Equipment Technology
ISO 2382-4	Vocabulary, Part 4: Organization of Data
ISO 2382-5	Vocabulary, Part 5: Representation of Data
ISO 2382-6	Vocabulary, Part 6: Preparation and Handling of Data
ISO/IEC 2382-7	Vocabulary, Part 7: Computer Programming
ISO 2382-8	Vocabulary, Part 8: Control, Integrity, and Security
ISO 2382-9	Vocabulary, Part 9: Data Communications
CD 2382-9.2	Vocabulary, Part 9: Data Communications, Edition 2
ISO 2382-10	Vocabulary, Part 10: Operating Techniques and Facilities
ISO 2382-11	Vocabulary, Part 11: Processing Units
ISO 2382-12	Vocabulary, Part 12: Peripheral Equipment
ISO 2382-13	Vocabulary, Part 13: Computer Graphics
ISO 2382-14	Vocabulary, Part 14: Reliability, Maintenance, and Availability
ISO 2382-15	Vocabulary, Part 15: Programming Languages
ISO 2382-16	Vocabulary, Part 16: Information Theory
DIS 2382-17	Vocabulary, Part 17: Databases
ISO 2382-18	Vocabulary, Part 18: Distributed Data Processing
ISO 2382-19	Vocabulary, Part 19: Analog Computing
ISO/IEC 2382-20	Vocabulary, Part 20: System Development
ISO 2382-21	Vocabulary, Part 21: Interfaces Between Process Computer Systems and Technical Processes
ISO 2382-22	Vocabulary, Part 22: Calculators
CD 2382-23	Vocabulary, Part 23: Text Processing
ISO/IEC 2382-25	Vocabulary, Part 25: Local Area Networks
DIS 2382-26	Vocabulary, Part 26: OSI Architecture
ISO 2955	Representation of SI and Other Units in Systems with Limited Character Sets
ISO 3166	Codes for the Representation of Names of Countries
ISO 3307	Representations of Time of the Day

ISO 3534	Statistics - Vocabulary and Symbols
ISO 4031	Information Interchange - Representation of Local Time Differentials
ISO 6093	Representation of Numeric Values in Character Strings for Information Exchange
ISO 6523	Data Interchange - Structure for the Identification of Organizations
	DAM1 Guidance on the Use of ISO 6523
ISO 6548	Data processing, Description of Interface Between Process Computing System and Technical Processes, 1984
ISO 6709	Standard Representation of Latitude, Longitude and Altitude for Geographic Point Locations
DTR 7352	Guidelines for Grouping of Data Elements in the Context of Data Interchange (being withdrawn)
DIS 7826-1	Representation of Data Elements, Part 1: Identification of Coding Schemes for Data Elements (Types), November 1993
DIS 7826-2	Representation of Data Elements, Part 2: Registration of Coding Schemes for Data Elements (Types), November 1993
ISO 8211	Specification for a Data Descriptive File for Information Interchange
DIS 8211.2	Specification for a Data Descriptive File for Information Interchange, Edition 2
ISO 8601	Representation of Dates and Times
ISO 8790	Computer System Configuration Diagram Symbols and Conventions
ISO/IEC 9282-1	Coded Representation of Pictures, Part 1: Encoding Principles for Picture Representation in a 7- or 8-Bit Environment
ISO/IEC 9282-2	Coded Representation of Pictures, Part 2: Encoding Principles for Photographic Images
ISO/IEC TR 9544	Computer-Assisted Publishing - Vocabulary
TR 9789	Guidelines for Data Interchange - Coding Methods and Principles, November 1993
WD 11179-1.3	Coordination of Data Elements, Part 1: Framework for the Generation and Standardization of Data Elements, November 1993
WD 11179-2.2	Coordination of Data Elements, Part 2: Classification of Concepts for the Identification of Domains, November 1993
DIS 11179-3	Coordination of Data Elements, Part 3: Data Element Attributes, November 1993
DIS 11179-4	Coordination of Data Elements, Part 4: Definition of Data Elements, Janaury 1994
CD 11179-5.2	Coordination of Data Elements, Part 5: Naming Principles for Data Elements, Janaury 1994
CD 11179-6	Coordination of Data Elements, Part 6: Representation of Data Elements (Types), November 1993
CD 11714	General Principles for the Creation of Symbols for Use in Technical Documentation of Products
ISO/IEC TR 12382	Permuted Index of the Vocabulary of Information Technology
CD 13522	Coded Representation of Multimedia and Hypermedia Information Objects
SC21 N 5394	Collections of Definitions of OSI Vocabulary

E. CODED CHARACTER SETS:

ISO 646	ISO 7-Bit Coded Character Set for Information Exchange
ISO 2022	ISO 7-Bit and 8-Bit Coded Character Sets - Code Extension Techniques
ISO 4873	8-Bit Code for Information Interchange - Structure and Rules for Implementation
ISO 6429	ISO 7-Bit and 8-Bit Coded Character Sets - Control Functions for Coded Character Sets
ISO 6936	Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2), Edition 2
ISO 6937-1	Coded Character Sets for Text Communication, Part 1: General Introduction
ISO 6937-2	Coded Character Sets for Text Communication, Part 2: Latin Alphabetic and Non-Alphabetic Graphic Characters
	AD 1 Addendum 1
DIS 6937-2.2	Coded Character Sets for Text Communication, Part 2: Latin Alphabetic and Non-Alphabetic Graphic Characters, Edition 2
DIS 6937-3	Coded Character Sets for Text Communication, Part 3: Control Functions for Page-Image Format
DIS 6937-7	Coded Character Sets for Text Communication, Part 7: Greek Graphic Characters
DIS 6937-8	Coded Character Sets for Text Communication, Part 8: Cyrillic Graphic Characters
ISO/IEC 7350	Registration of Graphic Character Subrepertoires
ISO 8859-1	8-Bit Single-Byte Coded Graphic Character Sets, Part 1: Latin Alphabet No. 1
ISO 8859-2	8-Bit Single-Byte Coded Graphic Character Sets, Part 2: Latin Alphabet No. 2
ISO 8859-3	8-Bit Single-Byte Coded Graphic Character Sets, Part 3: Latin Alphabet No. 3
ISO 8859-4	8-Bit Single-Byte Coded Graphic Character Sets, Part 4: Latin Alphabet No. 4
ISO/IEC 8859-5	8-Bit Single-Byte Coded Graphic Character Sets, Part 5: Latin/Cyrillic Alphabet
ISO 8859-6	8-Bit Single-Byte Coded Graphic Character Sets, Part 6: Latin/Arabic Alphabet
ISO 8859-7	8-Bit Single-Byte Coded Graphic Character Sets, Part 7: Latin/Greek Alphabet
ISO 8859-8	8-Bit Single-Byte Coded Graphic Character Sets, Part 8: Latin/Hebrew Alphabet
ISO/IEC 8859-9	8-Bit Single-Byte Coded Graphic Character Sets, Part 9: Latin Alphabet No. 5
ISO/IEC 8859-10	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 10: Latin/ Alphabet

ISO/IEC 9541-1	Font and Character Information Exchange, Part 1: Introduction
	Cor 1 Technical Corrigendum 1
ISO/IEC 9541-2	Font and Character Information Exchange, Part 2: Registration and Naming Procedures
DIS 9541-3	Font and Character Information Exchange, Part 3: Glyph Shape Representation
DIS 9541-4	Font and Character Information Exchange, Part 4: Character Collections
DIS 9541-5	Font and Character Information Exchange, Part 5: Font Attributes and Character Model
DIS 9541-6	Font and Character Information Exchange, Part 6: Font and Character Attribute Subsets and Application
DP 9541-7	Font and Character Information Exchange, Part 7: Font Interchange Format
ISO/IEC 10036	Procedure for Registration of Glyph and Glyph Collection Identifiers, 1993
ISO/IEC 10646	Multiple Octet Coded Character Set
ISO/TR 11065	Industrial Automation Glossary, 1992
ISO 11103	Space Data and Information Transfer Systems - Radio Metric and Orbit Data, 1991
ISO 11104	Space Data and Information Transfer Systems - Time Code Formats, 1991
SC21 N 8260	Liaison to SC21 on the Character, Graphic Symbol and Glyph, SC18/WG8, October 1993

F. MAN-MACHINE LANGUAGE (MML):

ITU-TS Z.301	Introduction to the CCITT Man-Machine Language (MML)
ITU-TS Z.302	The Meta-Language for Describing MML Syntax and Dialogue Procedures
ITU-TS Z.311	Introduction to Syntax and Dialogue Procedures (MML)
ITU-TS Z.312	Basic Format Layout (MML)
ITU-TS Z.314	The Character Set and Basic Elements (MML)
ITU-TS Z.315	Input (Command) Language Syntax Specification (MML)
ITU-TS Z.316	Output Language Syntax Specification (MML)
ITU-TS Z.317	Man-Machine Dialogue Procedures (MML)
ITU-TS Z.321	Introduction to the Extended MML for Visual Display Terminals
ITU-TS Z.322	Capabilities of Visual Display Terminals
ITU-TS Z.323	Man-Machine Interaction
ITU-TS Z.331	Introduction to the Specification of the Man-Machine Interface
ITU-TS Z.332	Methodology for the Specification of the Man-Machine Interface - General Working Procedures
ITU-TS Z.333	Methodology for the Specification of the Man-Machine Interface - Tools and Methods
ITU-TS Z.341	Glossary of Terms (MML)
ITU-TS Z.351	Data-oriented Human-Machine Interface Specification Techniques, Part 1: Introduction
ITU-TS Z.352	Data-oriented Human-Machine Interface Specification Techniques, Part 2: Scope, Approach and Reference Model

G. SOFTWARE DEVELOPMENT AND DOCUMENTATION:

ISO/TR 1286	Manufacturing Automation Programming Language Environment Architecture (MAPLE), 1993
ISO/IEC 1538	Programming Languages - ALGOL 60
ISO 1539	Programming Languages - FORTRAN
DIS 1539.2	Programming Languages - FORTRAN Extended
ISO 1989	Programming Languages - COBOL
	AM 1 Amendment 1: Intrinsic Function Module
ISO 6160	Programming Languages - PL/1
ISO 6373	Programming Languages - BASIC
ISO/IEC 6522	Programming Languages - PL/1 General Purpose Subset
ISO 6592	Guidelines for the Documentation of Computer-Based Application Systems
ISO 7185	Programming Languages - Pascal
ISO 8485	Programming Languages - APL
ISO 8631	Information Technology - Program Constructs and Conventions for Their Representation, 1989
ISO 8652	Programming Languages - Ada
ISO 9000	Quality Management and Quality Assurance Standards - Guidelines for Selection and Use, 1987
ISO 9000-3	Quality Management and Quality Assurance Standards, Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply, and Maintenance of Software, 1991
ISO 9001	Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation and Servicing, 1987
ISO 9002	Quality Systems - Model for Quality Assurance in Production and Installation, 1987
ISO 9003	Quality Systems - Model for Quality Assurance in Final Inspection and Test, 1987
ISO 9004	Quality Management and Quality System Elements - Guidelines, 1987
ISO 9004-2	Quality Management and Quality System Elements, Part 2: Guidelines for Services, 1991
ISO/IEC 9126	Information technology, Software Product Evaluation, Quality Characteristics and Guidelines for Their Use

ISO 9127	Information processing systems, User Documentation and Cover Information for Consumer Software Packages
ISO/IEC TR 9294	Guidelines for the Management of Software Documentation, Technical Report Type 3
ISO 9496	Programming Languages - CCITT High Level Language (CHILL)
ISO/TR 9547	Programming Language Processors - Test Methods - Guidelines for Their Development and Acceptability
ISO 9899	Programming Languages - C
ISO/IEC TR 10034	Guidelines for the Preparation of Conformity Clauses in Programming Language Standards
ISO/IEC TR 10176	Guidelines for the Preparation of Programming Language Standards
DTR 10182	Binding Techniques for Programming Languages
ISO/IEC 10206	Programming Languages Extended Pascal
ISO/IEC 10279	Programming Languages - Full BASIC
CD 10967-1	Programming Languages, Their Environments and Systems Software Interfaces - Language Compatible Arithmetic, Part 1: Integer and Floating Point Arithmetic
WD 10967-2	Programming Languages, Their Environments and Systems Software Interfaces - Language Compatible Arithmetic, Part 2: Complex Arithmetic and Mathematical Procedures
ISO/IEC 11404	Programming Languages - Common Language-Independent Data Types (CLID)
ISO/IEC 11756	Programming Languages, MUMPS
ISO/IEC 12119	Software Packages: Quality Requirements and Testing
DIS 13719-1	Portable Common Tools Environment (PCTE), Part 1: Abstract Specification (ECMA-149)
DIS 13719-2	Portable Common Tools Environment (PCTE), Part 2: C Programming Language Binding to PCTE (ECMA-158)
DIS 13719-3	Portable Common Tools Environment (PCTE), Part 3: Ada Programming Language Binding (ECMA-162)
SC21 N 6820	Liaison Statement for SC22/WG11, Binding Techniques, to SC21/WG6 RPC Rapporteur Group
SC21 N 8103 Rev.	Request from SC21 to JTC1 Concerning the "Fast Tracking" of the PCTE Document, June 1993
ITU-TS Z.200 Rev 1	ITU-TS High Level Language (CHILL)
ITU-TS Z.400	Structure and Format of Quality Manuals for Telecommunication Software

H. INFORMATION PROCESSING EQUIPMENT:

ISO 8884	Keyboards for Multiple Latin-Alphabet Languages - Layout and Operation Using Four Levels
ISO 9171-1	130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 1: Unrecorded Optical Disk Cartridge
ISO 9171-2	130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 2: Recording Format
ISO 9660	Volume and File Structure of CD-ROM for Information Exchange
DIS 9995-1	Keyboard Layouts for Text and Office Systems, Part 1: General Principles Governing Keyboard Layouts
DIS 9995-2	Keyboard Layouts for Text and Office Systems, Part 2: Alphanumeric Section
DIS 9995-3	Keyboard Layouts for Text and Office Systems, Part 3: Common Secondary Layout of Alphanumeric Zone of Alphanumeric Section
DIS 9995-4	Keyboard Layouts for Text and Office Systems, Part 4: Principles Governing the Placement of Characters and Symbols on Keys
DIS 9995-5	Keyboard Layouts for Text and Office Systems, Part 5: Editing Section
DIS 9995-6	Keyboard Layouts for Text and Office Systems, Part 6: Functional Section
DIS 9995-7	Keyboard Layouts for Text and Office Systems, Part 7: Symbols Used to Represent Functions
DIS 9995-8	Keyboard Layouts for Text and Office Systems, Part 8: Allocation of Letters to the Keys of a Numeric Keyboard
DP 10033	Recording of Documents Conforming to ISO 8613 on Flexible Disk Cartridges Conforming to ISO 9293
ISO 10149	Data Interchange on Read-Only 120-mm Optical Data Disks (CD-ROM)
DIS 10222	Enhanced Small Device Interface
DIS 10994	Data Interchange on 90 mm Flexible Disk Cartridges Using MFM Recording at 31,831 FTPRAD on 80 Tracks on Each Side
ISO/IEC 11319	8 mm Wide Magnetic Tape Cartridge for Information Interchange - Helical Scan Recording, 1993
DIS 11321	3,81 mm Wide Magnetic Tape Cartridge for Information Interchange - Helical Scan Recording - Data/Data Format, 1993

APPENDIX E

NUMERICAL LISTING OF ISO STANDARDS AND CCITT RECOMMENDATIONS RELEVANT TO CCISs

I. ISO Standards
II. CCITT Standards

NUMERICAL LISTING OF ISO/IEC STANDARDS AND ITU-TS (FORMERLY CCITT) RECOMMENDATIONS RELEVANT TO INFORMATION SYSTEMS[1]

I. ISO/IEC STANDARDS

ISO 646	Information Processing - ISO 7-Bit Coded Character Set for Information Exchange, Edition 3, 1991
IEC 847	Characteristics of LANs, 1988
IEC/TR 907	Local Area Networks CSMA/CD 10 Mbit/s Baseband Planning and Installation Guide, 1989
ISO 1155	Information Processing - Use of Longitudinal Parity to Detect Errors in Information Messages, Edition 2, 1978
ISO/TR 1286	Manufacturing Automation Programming Language Environment Architecture (MAPLE), 1993
ISO 1177	Information Processing - Character Structure for Start/Stop and Synchronous Character Oriented Transmission, Edition 2, 1985
ISO/IEC 1538	Information Technology - Programming Languages - ALGOL 60, 1984
ISO 1539	Programming Languages - FORTRAN, Edition 2, 1991
DIS 1539.2	Programming Languages - FORTRAN Extended, 1991
ISO 1745	Information Processing - Basic Mode Control Procedures for Data Communication Systems, February 1975
ISO 1989	Programming Languages - COBOL (Endorsement of ANSI Standard X3.53-1976), Edition 2, 1985
ISO 1989 AM 1	Amendment 1, Intrinsic Function Module, 1992
ISO 2022	Information Processing - ISO 7-Bit and 8-Bit Coded Character Sets - Code Extension Techniques, Edition 3, May 1986
ISO 2110♦[2]	Information Technology - Data Communication - 25-Pin DTE/DCE Interface Connector and Contact Number Assignments, Edition 3, 10 April 1989
ISO 2110 AM 1	Amendment 1, Interface Connector and Contact Number Assignments for a DTE/DCE for Data Signalling Rates Above 20 kbit/s, April 1991
ISO 2111	Data Communication - Basic Mode Control Procedures - Code Independent Information Transfer, Edition 2, February 1985
ISO 2375	Data Processing - Procedures for the Registration of Escape Sequences, Edition 3, November 1985
ISO 2382-1	Data Processing - Vocabulary, Part 1: Fundamental Terms, Edition 2, 1984
ISO 2382-2	Data Processing - Vocabulary, Part 2: Arithmetic and Logic Operations, 1976
ISO 2382-3	Information Processing Systems - Vocabulary, Part 3: Equipment Technology, Edition 2, 1987
ISO 2382-4	Information Processing Systems - Vocabulary, Part 4: Organization of Data, Edition 2, 1987
ISO 2382-5	Information Processing Systems - Vocabulary, Part 5: Representation of Data, Edition 2, 1989
ISO 2382-6	Information Processing Systems - Vocabulary, Part 6: Preparation and Handling of Data, Edition 2, 1987
ISO/IEC 2382-7	Information Processing Systems - Vocabulary, Part 7: Computer Programming, Edition 2, 1989
ISO 2382-8	Information Processing Systems - Vocabulary, Part 8: Control, Integrity, and Security, 1986
ISO 2382-9	Data Processing - Vocabulary, Part 9: Data Communication, March 1984
CD 2382-9.2	Data Processing - Vocabulary, Part 9: Data Communication, Edition 2, April 1991
ISO 2382-10	Data processing - Vocabulary, Part 10: Operating Techniques and Facilities, 1979
ISO 2382-11	Information Processing Systems - Vocabulary, Part 11: Processing Units, Edition 2, 1987
ISO 2382-12	Information Processing Systems - Vocabulary, Part 12: Peripheral Equipment, Edition 2, 1988
ISO 2382-13	Data Processing - Vocabulary, Part 13: Computer Graphics, 1984
ISO 2382-14	Data Processing - Vocabulary, Part 14: Reliability, Maintenance, and Availability, 1978

---

1 Based on data initially provided by OMNICON in September 19[illegible] Revised based on:
  a. *ISO/IEC JTC1/SC 21 Programme of Work* [SC21 N 8082 19[illegible]]
  b. *ISO Catalogue* [ISO 1993]
  c. November 1993 *Directory of ISPs and Profiles Contained Therein*, SGFS SD-4 [SGFS N 1049]
  d. September 1993 *NOSIP Strategy* [NATO 1993]
  e. Private communication from UK's Defence Research Agency [DRA 1993]
  f. Additional contributions from the nations participating in the ATCCIS PWG.

2 The symbol ♦ is used throughout this appendix to identify those standards included in the September 1993 *NOSIP Strategy* [Ref. NATO 1993].

ISO 2382-15	Data Processing - Vocabulary, Part 15: Programming Languages, 1985
ISO 2382-16	Data Processing - Vocabulary, Part 16: Information Theory, 1978
DIS 2382-17	Data Processing - Vocabulary, Part 17: Databases, 17 October 1993 (ballot ends April 1994)
ISO 2382-18	Information Processing Systems - Vocabulary, Part 18: Distributed Data Processing, 1987
ISO 2382-19	Information Processing Systems - Vocabulary, Part 19: Analog Computing, Edition 2, 1989
ISO/IEC 2382-20	Information Processing Systems - Vocabulary, Part 20: System development, 1990
ISO 2382-21	Information Processing Systems - Vocabulary, Part 21: Interfaces Between Process Computer Systems and Technical Processes, 1985
ISO 2382-22	Information Processing Systems - Vocabulary, Part 22: Calculators, 1986
CD 2382-23	Data Processing - Vocabulary, Part 23: Text Processing, January 1991
ISO/IEC 2382-25	Data Processing - Vocabulary, Part 25: Local Area Networks, 1992
DIS 2382-26	Data Processing - Vocabulary, Part 26: OSI Architecture, January 1992 (ballot ended December 1992)
ISO 2593:1984◆	Data Communication - 34-Pin DTE/DCE Open Systems Interface Connector and Pin Assignments, Edition 2, 1984
DIS 2593.3	Data Communication - 34-Pin DTE/DCE Open Systems Interface Connector and Pin Assignments, Edition 3, 1992
ISO 2628	Basic Mode Control Procedures - Complements, June 1973
ISO 2629	Basic Mode Control Procedures - Conversational Information Message Transfer, February 1973
ISO 2955	Information Processing - Representation of SI and Other Units in Systems with Limited Character Sets, 1983 (reviewed in 1993 by JTC1/SC14)
ISO 3166	Codes for the Representation of Names of Countries, Edition 3, 1988 (ANSI/NISO/ISO 3166-1991)
ISO 3307	Information Interchange - Representations of Time of the Day, March, 1975
ISO 3309:1984◆	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Frame Structure, Edition 3, June 1991
ISO 3309:1991	Information Technology - Telecommunication and Information Exchange Between Systems - High-Level Data Link Control (HDLC) Procedures - Frame Structure, Edition 4, June 1991
ISO 3309:1991 AM 2◆	Amendment 2: Extended Transparency Option for Start/Stop Transmission, 1992
ISO 3309:1991 PDAM 3	Amendment 3: Seven-bit Transparency Option for Start/Stop Transmission, 1991
ISO 3534	Statistics - Vocabulary and Symbols, 1977
ISO 4031	Information Interchange - Representation of Local Time Differentials, December 1987
ISO 4335:1984◆	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures, Elements of Procedures, Edition 3, 1984
ISO/IEC 4335:1991	Information Technology - Telecommunication and Information Exchange Between Systems - High-Level Data Link Control (HDLC) Procedures, Elements of Procedures, Draft Edition 4, 1991
ISO/IEC 4335:1991 AM 4	Amendment 4: Multi-Selective Reject, 1989
ISO/IEC 4335:1991 PDAD 5	Addendum 5: Flow Control Unnumbered Information (FUI), January 1991
ISO 4873	Information Technology - 8-Bit Code for Information Interchange - Structure and Rules for Implementation, Edition 2, July 1991 (ANSI/ISO 4871-1991)
ISO 4902◆	Information Technology - Data Communication - 37-Pole DTE/DCE Interface Connector and Contact Number Assignments, Edition 2, 1989
ISO 4903◆	Information Technology - Data Communication - 15-Pole DTE/DCE Interface Connector and Contact Number Assignments, Edition 2, 1989
ISO 5807	Information Processing - Documentation Symbols and Conventions for Data, Program and System Flowcharts, Program Network Charts and System Resource Charts, 1985 (ANSI/ISO 5807-1985)
ISO 6093	Information Processing Systems - Representation of Numeric Values in Character Strings for Information Exchange, November 1985 (Reaffirmed July 1991)
ISO 6160	Programming Languages - PL/1 (Endorsement of ANSI Standard X3.53-1976), 1979
ISO 6373	Data Processing - Programming Languages - Minimal BASIC, 1984
ISO 6429	ISO 7-Bit and 8-Bit Coded Character Sets - Control Functions for Coded Character Sets, 1992
ISO/IEC 6522	Information Technology - Programming Languages - PL/1 General Purpose Subset, Edition 2, 1992
ISO 6523	Data Interchange - Structure for the Identification of Organizations, February 1984
ISO 6523 DAM 1	Guidance on the Use of ISO 6523, 1993 (IS status expected early in 1994)
ISO 6548	Data Processing - Description of Interface Between Process Computing System and Technical Process, 1984
ISO 6592	Information Processing - Guidelines for the Documentation of Computer-Based Application Systems, November 1985
ISO 6709	Standard Representation of Latitude, Longitude and Altitude for Geographic Point Locations, 1983 (reviewed by JTC1/SC14 in 1993)
ISO 6936	Information Processing - Conversion Between the Two Coded Character Sets of ISO 646 and ISO 6937-2 and the CCITT International Telegraph Alphabet No. 2 (ITA2), Edition 2, 1988
ISO 6937-1	Information Processing - Coded Character Sets for Text Communication, Part 1: General Introduction, November 1983

ISO 6937-2	Information Processing - Coded Character Sets for Text Communication, Part 2: Latin Alphabetic and Non-Alphabetic Graphic Characters, December 1983
ISO 6937-2 AD 1	Addendum 1, 1989
DIS 6937-2.2	Information Processing - Coded Character Sets for Text Communication, Part 2: Latin Alphabetic and Non-Alphabetic Graphic Characters, Edition 2, October 1991
DIS 6937-3	Information Processing - Coded Character Sets for Text Communication, Part 3: Control Functions for Page-Image Format, March 1988
DIS 6937-7	Information Processing - Coded Character Sets for Text Communication, Part 7: Greek Graphic Characters, April 1987
DIS 6937-8	Information Processing - Coded Character Sets for Text Communication, Part 8: Cyrillic Graphic Characters, April 1987
ISO 6951	Information Processing - Processor System Bus Interface (Eurobus A), 1986
ISO 7185	Information Technology - Programming Languages - Pascal, Edition 2, 1990 (ANSI/ISO 7185-1990)
ISO/IEC 7350	Information Technology - Registration of Repertoires of Graphic Characters from ISO 10367, Edition 2, 1991
DTR 7352	Information Technology - Guidelines for Grouping of Data Elements in the Context of Data Interchange (JTC1/SC14 recommended in November 1993 that this draft technical report be withdrawn)
ISO/TR 7477◆	Data Communication - Arrangements for DTE to DTE Physical Connection Using V.24 and X.24 Interchange Circuits, September 1985
ISO 7478◆	Information Processing Systems - Data Communication - Multilink Procedures, July 1987
ISO 7478/Cor 1	Technical Corrigendum 1, 1 March 1989 [SC21 N 2738, June 1988]
ISO/IEC 7480	Information Technology - Telecommunications and Information Exchange Between Systems - Start-Stop Transmission Signal Quality at DTE/DCE Interfaces, Edition 2, October 1991
ISO 7498:1984	Information Processing Systems - Open Systems Interconnection - Basic Reference Model, October 1984 [SC21 N 3273, December 1988] (revision incorporating AD 1 is 7498-1 below) (X.200)
ISO 7498/Cor 1	Technical Corrigendum 1, 15 December 1988
ISO 7498 AD 1◆	Addendum 1: Connectionless-Mode Transmission, July 1987
ISO 7498 PDAD 2	Addendum 2: Multipeer Data Transmission (MPDT) [SC21 N 3287] (Reassessed in SC21 N 3906, September 1989; project suspended in November 1989 per SC21 N 4276; comments on reactivation of project requested in SC21 N 6197)
ISO/IEC 7498-1:1994◆	Information Technology - Open Systems Interconnection - Basic Reference Model, Part 1: General Aspects, Edition 2, 1994 [SC21 N 8228]
ISO 7498-2◆	Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Part 2: Security Architecture, February 1989 (X.800:1991)
ISO 7498-3◆	Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Part 3: Naming and Addressing, March 1989 (X.650:1992)
ISO/IEC 7498-4◆	Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Part 4: Management Framework, November 1989 [SC21 N 3502] (X.700:1992)
WD 7498-5	Information Processing Systems - Open Systems Interconnection - Basic Reference Model, Part 5: Architecture for Multi-Peer Communications, August 1993 [SC21 N 8003] (ballot ends November 1993; CD expected in 1996)
ISO 7776◆	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Description of the X.25 LAPB-Compatible DTE Data Link Procedures, December 1986
ISO 7776/Cor 1	Technical Corrigendum 1, 1 April 1989
ISO 7776/Cor 2	Technical Corrigendum 2, 1 September 1989
ISO 7776/Cor 3	Technical Corrigendum 3, 1991
ISO 7776 AM 1	Amendment 1: Conformance Requirements, 1992
ISO 7809:1984◆	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - Classes of Procedures, Edition 1, 1984
ISO/IEC 7809:1991	Information Technology - Telecommunications and Information Exchange Between Systems - High-Level Data Link Control (HDLC) Procedures - Classes of Procedures, Edition 2, January 1991
ISO/IEC 7809:1991 AM 5	Amendment 5: Connectionless Class of Procedures, 1992
ISO/IEC 7809:1991 AM 6	Amendment 6: Extended Transparency Options for Start/Stop Transmission, 1992
ISO/IEC 7809:1991 AM 7	Amendment 7: Multi-Selective Reject Option, January 1991
ISO/IEC 7809:1991 PDAM 9	Amendment 9: Seven-bit Transparency Option for Start/Stop Transmission, 1991
ISO 7816-1	Information Technology - Identification Cards - Identification Cards with Contacts, Part 1: Physical Characteristics, 1987, SC17/WG (ANSI/ISO 7816/1-1987)
ISO 7816-2	Information Technology - Identification Cards - Identification Cards with Contacts, Part 2: Number and Position of Contacts 1988, SC17/WG (ANSI/ISO 7816/2-1988)
ISO 7816-3	Information Technology - Identification Cards - Identification Cards with Contacts, Part 3: Electronic Signals/Exchange Protocols, SC17/WG4

DIS 7826-1	Information Technology - Representation of Data Elements, Part 1: Identification of Coding Schemes for Data Elements (Types), November 1993 (balloting ended February 1994)
DIS 7826-2	Information Technology - Representation of Data Elements, Part 2: Registration of Coding Schemes for Data Elements (Types), November 1993 (balloting ended February 1994)
ISO 7846	Industrial Real-time FORTRAN Application for the Control of Industrial Processes, 1985
ISO 7942	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Functional Description, August 1985
ISO 7942 AM 1	Amendment 1: Audit Trail Metafile, 1991
ISO 8072◆	Information Processing Systems - Open Systems Interconnection - Transport Service Definition, June 1986 (ANSI/ISO 8072-1986)
ISO 8072/Cor 1	Technical Corrigendum 1, 1991
ISO 8072 AD 1	Addendum 1: Connectionless-Mode Transmission, July 1986
ISO/IEC 8073◆	Information Processing Systems - Telecommunications and Information Exchange Between Systems - Protocol for Providing the Connection-mode Transport Service, Edition 3, 1992
ISO/IEC 8208◆	Information Processing Systems - Data Communications - X.25 Packet Level Protocol (PLP) for Data Terminal Equipment, Edition 2, March 1990
ISO/IEC 8208/Cor 1	Technical Corrigendum 1, 1992
ISO/IEC 8208 AM 1	Amendment 1: Alternative Logical Channel Identifier Assignment, September 1990
ISO/IEC 8208 PDAD 2	Addendum 2 - Extensions for Private and Switched Use (project canceled; WITHDRAWN, 1989)
ISO/IEC 8208 AM 3	Amendment 3: Conformance Requirements, February 1991
ISO 8211	Information Processing - Specification for a Data Descriptive File for Information Interchange, December 1985 (ANSI/ISO 8211-1985)
DIS 8211.2	Information Processing - Specification for a Data Descriptive File for Information Interchange, Edition 2, January 1993 [SC21 N 7555] (passed ballot in October 1993)
ISO 8326◆	Information Processing Systems - Open Systems Interconnection - Connection Oriented Session Service Definition, Revised Edition, 1990 (incorporated AD 1, AD 2, and AD 3) (X.215)
ISO 8326 AM 4	Addendum 4: Additional Synchronization Functionality, December 1992
ISO 8326 WDAM 5	Addendum 5: Removal of Session Layer Serial Number Limitation, August 1993 [SC21 N 7929] (rapporteur meeting December 1993; PDAM expected July 1994)
DIS 8326.2	Information Processing Systems - Open Systems Interconnection - Connection Oriented Session Service Definition, Edition 2, September 1993 [SC21 N 8207] (X.215)
ISO 8327◆	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification, Revised Edition 1990 (incorporated AD 1 and AD 2) (X.225)
ISO 8327 AM 3	Amendment 3 to Incorporate Additional Synchronization Functionality, December 1992 [SC21 N 7261]
ISO 8327 WDAM 4	Amendment 4: Removal of Session Layer Serial Number Limitation, August 1993 [SC21 N 7929] (rapporteur meeting December 1993; PDAM expected July 1994)
DIS 8327-1	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Session, Part 1: Protocol Specification, Edition 2 of ISO 8327, September 1993 [SC21 N 8208] (X.225)
ISO 8327-2◆	Information Technology - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification, Part 2: Protocol Implementation Conformance Statement (PICS) Proforma, 1993 (X.245)
ISO 8348:1993◆	Information Processing Systems - Data Communications - Network Service Definition, Edition 2, 1993
ISO 8372	Information Processing - Modes of Operation for a 64-bit Block Cipher Algorithm, 1987
ISO 8471◆	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Balanced Classes of Procedures - Data-Link Layer Address Resolution/Negotiation in Switched Environments, April 1987
ISO 8473◆	Information Processing Systems - Data Communication - Protocol for Providing the Connectionless-Mode Network Service (CLNS), January 1988
ISO 8473/Cor 1	Technical Corrigendum 1, 1992
ISO 8473 PDAD 1	Addendum 1: Provision of Underlying Service Assumed by ISO 8473 over Point-to-Point Subnetworks which Provide the OSI Data Link Service, July 1987 (DP)
ISO 8473 PDAD 2	Addendum 2: Estelle Formal Description of ISO 8473, Revised Edition, April 1988 (to be reballoted as a DTR)
ISO 8473 AD 3	Addendum 3: Provision of the Underlying Service Assumed by ISO 8473 over Subnetworks which Provide the OSI Data Link Service, September 1989
ISO 8473 PDAM 4	Amendment 4: PICS Proforma (new work item)
ISO 8473 DAM 5◆	Amendment 5: Provision of the Underlying Service Assumed by ISO 8473 over ISDN Circuit-Switched B-channels, August 1991
ISO 8480	Information Processing - Data Communication - DTE/DCE Interface Back-up Control Operation Using the 25-Pole Connector, November 1987
ISO 8481◆	Data Communication - DTE to DTE Physical Connection Using X.24 Interchange Circuits with DTE Providing Timing, September 1986

ISO 8482•	Information Processing Systems - Data Communication - Twisted Pair Multipoint Interconnections, November 1987
ISO 8485	Programming Languages - APL, 1989
DIS 8505	Information Processing Systems - Text Communication - Functional Description and Service Specification for Message Oriented Text Interchange Systems (MOTIS), February 1986 (WITHDRAWN, superseded by ISO 10021)
ISO/TR 8509•	Information Processing Systems - Open Systems Interconnection - Service Conventions, September 1987 (X.210:1988; see ISO 10731)
ISO 8571-1•	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 1: General Introduction, Revised Edition, October 1988
ISO 8571-1/Cor 1	Technical Corrigendum 1, June 1991
ISO 8571-1 AM 1	Amendment 1: Filestore Management, December 1992
ISO 8571-1 AM 2	Amendment 2: Overlapped Access, August 1993
ISO 8571-1 AM 3	Amendment 3: Service Enhancement, December 1993
ISO 8571-1 WDAM 4	Amendment 4: Enhanced Security for FTAM, May 1993 [SC21 N 7927] (project suspected in July 1993 pending resource availability and stability of GULS)
WD 8571-1.2	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 1: General Introduction, Edition 2 (WD expected January 1994; IS expected December 1994)
ISO 8571-2•	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 2: Virtual Filestore Definition, Revised Edition, October 1988
ISO 8571-2/Cor 1	Technical Corrigendum 1, June 1991
ISO 8571-2 AM 1	Amendment 1: Filestore Management, December 1992
ISO 8571-2 AM 2	Addendum 2: Overlapped Access, August 1993
ISO 8571-2 PDAM 3	Amendment 3: Enhancement for FTAM Services to Satisfy Additional User Requirements, March 1992 [SC21 N 6787] (project suspected in 1993)
ISO 8571-2 WDAM 4	Amendment 4: Enhancement to FTAM Security Services (project suspended in 1993)
WD 8571-2.2	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 2: Virtual Filestore Definition, Edition 2 (WD expected January 1994; IS expected December 1994)
ISO 8571-3•	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 3: File Service Definition, Revised Edition, October 1988
ISO 8571-3/Cor 1	Technical Corrigendum 1, June 1991]
ISO 8571-3/Cor 2	Technical Corrigendum 2, October 1992
ISO 8571-3 AM 1	Amendment 1: Filestore Management, December 1992
ISO 8571-3 AM 2	Addendum 2: Overlapped Access, August 1993
ISO 8571-3 AM 3	Amendment 3: Service Enhancement, December 1993
ISO 8571-3 WDAM 4	Amendment 4: Enhancement to FTAM Security Services (Project suspended)
WD 8571-3.2	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 3: File Service Definition, Edition 2 (WD expected January 1994; IS expected December 1994)
ISO 8571-4•	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 4: File Protocol Specification, Revised Edition, October 1988
ISO 8571-4/Cor 1	Technical Corrigendum 1, October 1992
ISO 8571-4 AM 1	Amendment 1: Filestore Management, December 1992
ISO 8571-4 AM 2	Addendum 2: Overlapped Access, August 1993
ISO 8571-4 AM 3	Amendment 3: Service Enhancement, December 1993
ISO 8571-4 AM 4	Amendment 4: Defect Report Changes, November 1992
ISO 8571-4 WDAM 5	Amendment 5: Enhanced Security to FTAM, 1992 (project suspected in 1993)
WD 8571-4.2	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 4: File Protocol Specification, Edition 2 (WD expected January 1994; IS expected December 1994)
ISO/IEC 8571-5•	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 5: Protocol Implementation Conformance Statement Proforma, Revised Edition, December 1990
ISO/IEC 8571-5 PDAM 1	Amendment 1: Filestore Management, May 1992 [SC21 N 7157] (editing meeting January 1994)
ISO/IEC 8571-5 WDAM 2	Amendment 2: Overlapped Access, June 1991 [SC21 N 6274] (undergoing reassessment; in the absence of an editor and target dates, SC21 is considering canceling this project)
ISO/IEC 8571-5 WDAM 3	Amendment 3: Enhancement for FTAM Services to Satisfy Additional User Requirements, June 1991 [SC21 N 6223] (to be progressed as a technical corrigendum)
ISO/IEC 8571-5 WDAM 4	Amendment 4: Enhancement to FTAM Security Services (project suspected in 1993)
WD 8571-5.2	Information Processing Systems - Open Systems Interconnection - File Transfer, Access and Management (FTAM), Part 5: Protocol Implementation Conformance Statement Proforma, Edition 2 (WD expected January 1994; IS expected December 1994)

ISO 8601	Data Elements and Interchange Formats - Information Exchange - Representation of Dates and Times, 1988
ISO 8602•	Information Processing Systems - Open Systems Interconnection - Protocol for Providing the Connectionless-Mode Transport Service, December 1987
ISO 8602 DAM 1	Amendment 1: PICS Proforma
ISO 8613-1•	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 1: Introduction and General Principles, July 1988 [T.411]
ISO 8613-1 AM 1	Amendment 1: Document Application Profile Proforma and Notation, 1993
ISO 8613-1 AM 2	Amendment 2: Conformance Testing Methodology, 1993
ISO 8613-2•	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 2: Document Structures, 1989 [T.412]
ISO 8613-2 PDAD 1	Addendum 1: Formal Specification of ODA Document Structures
DIS 8613-3	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 3: Abstract Interface for Manipulation of ODA Documents, April 1993
ISO 8613-4•	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 4: Document Profile, 1989 [ITU-TS T.414]
ISO 8613-5•	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 5: Office Document Interchange Format (ODIF), 1989 [T.415]
ISO 8613-6•	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 6: Character Content Architectures, 1989 [T.416]
ISO 8613-7•	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 7: Raster Graphics Content Architectures, 1989 [T.417]
ISO 8613-8•	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 8: Geometric Graphics Content Architectures, 1989 [T.418]
ISO 8613-8 DAD 1	Addendum 1: Tiled Raster Graphics, March 1990
ISO 8613-8 DAM 2.2	Amendment 2: Color, November 1990
ISO 8613-8 DAD 3	Addendum 3: Alternative Representation, March 1990
ISO 8613-8 DAD 4	Addendum 4: Security, March 1990
ISO 8613-8 DAM 5.2	Amendment 5: Streams, August 1991
ISO 8613-8 DAD 6	Addendum 6: Styles Extension, March 1990
ISO 8613-8 PDAM 10	Amendment 10: ODA External References and Document Fragments
CD 8613-9	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 9: Audio Content Architectures
ISO/IEC 8613-10	Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format, Part 10: Formal Specifications, 1991
ISO/IEC 8613-10 AM 1	Amendment 1: Formal Specification of the Document Profile (ballot closed 1 March 1991)
ISO/IEC 8613-10 AM 2	Amendment 2: Formal Specification of the Raster Graphics Content Architectures (ballot closed 1 March 1991)
ISO/IEC 8613-10 AM 3	Amendment 3: Formal Specification of ODA Character Content Architectures, 1992
ISO/IEC 8613-10 AM 4	Amendment 4: Formal Specification of ODA Geometric Graphics Content Architectures, 1992
ISO/IEC 8613-10 AM 5	Amendment 5: Formal Specification of the Defaulting Mechanism for Defaultable Attributes, 1993
CD 8613-11	ODA Spreadsheet, April 1993
DIS 8613-12	ODA Identification of Document Fragments, April 1993
ISO/IEC 8631	Information Technology - Program Constructs and Conventions for Their Representation, 1989
ISO/IEC 8632-1	Information Technology - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 1: Functional Specification, Edition 2, 1992
ISO/IEC 8632-1 AM 1	Amendment 1: Audit Trail Metafile, 1990
ISO/IEC 8632-1 PDAD 2	Addendum 2: 3D Static Picture Capture Metafile, 1989
ISO/IEC 8632-1 DAM 3	Amendment 3, January 1991
ISO/IEC 8632-1 DAM 4	Amendment 4: Rules for Profiles
ISO/IEC 8632-2	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 2: Character Encoding, Edition 2, 1992
ISO/IEC 8632-2 AM 1	Amendment 1, 1990
ISO/IEC 8632-2 DAM 3	Addendum 3, January 1991
ISO/IEC 8632-3	Information Processing Systems - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 3: Binary Encoding, Edition 2, 1992
ISO/IEC 8632-3 AM 1	Amendment 1, 1990
ISO/IEC 8632-3 DAM 3	Amendment 3, January 1991
ISO/IEC 8632-4	Information Technology - Computer Graphics - Metafile (CGM) for the Storage and Transfer of Picture Description Information, Part 4: Clear Text Encoding, Edition 2, 1992
ISO 8648•	Information Processing Systems - Open Systems Interconnection - Internal Organization of the Network Layer, February 1988
ISO 8648/Cor 1	Technical Corrigendum 1, 1991

ISO 8649:1988◆	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE), December 1988
ISO 8649:1992	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE), Revised Edition, April 1992 (incorporates AM 1 and AM 2) (X.217:1992)
ISO 8649:1992 DAM 3	Amendment 3: Application-Context Management Service, September 1993 [SC21 N 8046]
ISO 8649 WDAM 4	Amendment 4: Extensions to Support the Extended Application Layer Structure, December 1993 [SC21/WG8 N 194]
DIS 8649.2	Information Processing Systems - Open Systems Interconnection - Service Definition for the Association Control Service Element (ACSE), Edition 2 (IS expected November 1994) (X.217)
ISO 8650:1988◆	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE), December 1988
ISO 8650:1992	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE), Revised Edition, April 1992 (incorporates AM 1) (X.227:1992)
ISO 8650:1992 DAM 2	Amendment 2: Application Context Negotiation During Association Establishment, September 1993 [SC21 N 8047]
ISO 8650:1992 WDAM 3	Amendment 3: A-Context Management Service (formal WD text expected June 1992, CDAM in June 1993, DAM June 1994, AM in June 1995)
ISO 8650 WDAM 4	Amendment 4: Extensions to Support the Extended Application Layer Structure, December 1993 [SC21/WG8 N 195]
DIS 8650-1	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE), Edition 2 of ISO 8650 (IS expected November 1994) (X.227)
ISO 8650-2◆	Information Processing Systems - Open Systems Interconnection - Protocol Specification for the Association Control Service Element (ACSE), Part 2: PICS Proforma, 1993 [SC21 N 7003] (X.247)
ISO 8651-1	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Language Bindings, Part 1: FORTRAN, October 1988
ISO 8651-2	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Language Bindings, Part 2: Pascal, October 1988
ISO 8651-3	Information Processing Systems - Computer Graphics - Graphical Kernel System (GKS) Language Bindings, Part 3: Ada, October 1988
ISO/IEC 8651-4	Information Technology - Computer Graphics - Graphical Kernel System (GKS) Language Bindings, Part 4: C, 1991
ISO 8652	Programming Languages - Ada (Endorsement of ANSI Standard 1815A-1983), 1987
ISO 8730	Financial Transactions - Wholesale Banking Security - Requirements for Message Authentication, TC68/SC2
ISO 8731-1	Financial Transactions - Wholesale Banking Security - Approved Algorithms for Message Authentication, Part 1: DEA-1 Algorithm, TC68/SC2
ISO 8731-2	Financial Transactions - Wholesale Banking Security - Approved Algorithms for Message Authentication, Part 2: Message Authentication Algorithm, TC68/SC2
ISO 8732	Financial Transactions - Wholesale Banking Security - Key Management, TC68/SC6
ISO 8790	Information Processing Systems - Computer System Configuration Diagram Symbols and Conventions, September 1987
DP 8800-1	Information Resource Dictionary System (IRDS), Part 1: Command Language and Panel Interface (project cancelled)
ISO 8802-1◆	Information Processing Systems - Local Area Networks, Part 1: General Introduction, 1989
DIS 8802-1.2	Information Processing Systems - Local Area Networks, Part 1: General Introduction with System Load Protocol, November 1991
ISO 8802-2◆	Information Processing Systems - Local Area Networks, Part 2: Logical Link Control, 1989 [ANSI/IEEE 802.2-1989]
DIS 8802-2.2	Information Processing Systems - Local Area Networks, Part 2: Logical Link Control, Edition 2, July 1990
ISO 8802-2.2/Cor 1	Technical Corrigendum 1, 1992
DIS 8802-2.2 DAM 1	Amendment 1: Flow Control Techniques for Bridged Local Area Networks, May 1988
DIS 8802-2.2 DAM 2	Amendment 2: Type 3 Operation-Acknowledge Connectionless Service, June 1990
DIS 8802-2.2 DAM 3◆	Amendment 3: PICS Proforma, October 1991
DIS 8802-2.2 DAM 4	Amendment 4: Editorial Changes and Technical Corrections, May 1990
DIS 8802-2.2 PDAM 5	Amendment 5: Bridged LAN Source Routing Operations by End Systems, August 1991
ISO/IEC 8802-3◆	Information Technology - Local and Metropolitan Area Networks, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Edition 3, 1992 [ANSI/IEEE 802-3-1992]
ISO/IEC 8802-3 DAM 6	Amendment 6: Summary of IEEE 802.3, August 1991
ISO/IEC 8802-3 DAM 7	Amendment 7: LAN Layer Management, October 1991

ISO/IEC 8802-3 DAM 9	Amendment 9: Twisted Pair, Medium Attachment Unit, and Baseband Medium Specifications, Type 10 BASE-T, September 1991
ISO/IEC 8802-3 PDAM 11	Amendment 11: Hub Management, March 1992
ISO/IEC 8802-3 PDAM 13	Amendment 13: Attachment Unit Interface Cable Conformance Test, March 1992
ISO/IEC 8802-3 PDAM 15	Amendment 15: Corrections and Updates 2 & 3, March 1992
ISO/IEC 8802-3 PDAM 17	Amendment 17: PICS Proforma for 10 BASE-T, March 1992
ISO/IEC 8802-4◆	Information Technology - Local Area Networks, Part 4: Token-Passing Bus Access Method and Physical Layer Specifications, Edition 2, August 1990 [ANSI/IEEE 802-4-1990]
ISO/IEC 8802-5◆	Information Technology - Local and Metropolitan Area Networks, Part 5: Token Ring Access Method and Physical Layer Specification, Revised Edition containing Part 5 and its first 3 addenda, 1992 [ANSI/IEEE 802-5-1991]
DIS 8802-6◆	Information Processing Systems - Local Area Networks, Part 6: Distributed Queue Dual Bus (DQDB) Media Access Control (MAC), August 1991
ISO 8802-7	Information Technology - Local Area Networks, Part 7: Slotted Ring Access Method and Physical Layer Specification, 1991
DIS 8802-9◆	Information Processing Systems - Local Area Networks, Part 9: Integrated Voice and Data (IVD) Local Area Network
CD 8802-51	Information Processing Systems - Local Area Networks, Part 51: MAC Sublayer Conformance Test Purposes, December 1991
ISO 8805	Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Functional Description, October 1988
ISO 8805 WDAD 1	Addendum 1: Name Set Addendum, April 1987 (WD)
DIS 8806-1	Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Language Bindings, Part 1: FORTRAN, November 1988
DIS 8806-3	Information Processing Systems - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Language Bindings, Part 3: Ada, 1989
ISO/IEC 8806-4	Information Technology - Computer Graphics - Graphical Kernel System for Three Dimensions (GKS-3D) Language Bindings, Part 4: C, 1991
ISO 8807	Information Processing Systems - Open Systems Interconnection - LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour, February 1989 (Z.100)
ISO 8807 AM 1	Addendum 1, Graphical Representation of LOTOS (G-LOTOS), 1993 [SC21 N 6751]
ISO 8807 WDAM 2	Amendment 2: Enhancements to LOTOS, July 1993 [SC21 N 8023) (new work item ballot ends November 1993; rapporteur meeting January 1994; PDAM expected June 1995)
ISO 8822◆	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Service Definition, August 1988 (X.216)
ISO 8822 AM 1◆	Amendment 1: Connectionless-Mode Presentation Service, September 1991
ISO 8822 AM 2	Amendment 2: Unlimited User Data, 1993 [SC21 N 7419]
ISO 8822 DAM 3	Amendment 3: Abstract Syntax Registration, January 1993 [SC21 N 7556]
ISO 8822 AM 4	Amendment 4: Support of Session Symmetric Synchronization Service, November 1993
ISO 8822 AM 5	Amendment 5: Delivery of Additional Session Synchronization Functionality to the Presentation Service User, December 1992
DIS 8822.2	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Service Definition, Edition 2, August 1993 [SC21 N 8173] (incorporates AM1 to AM5) (X.216)
ISO 8823◆	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, August 1988 [SC21 N 2336, April 1988] (defect reports SC21 N 3751-3760, August 1989) (X.226)
ISO 8823 AM 2	Amendment 2: Unlimited User Data, 1993 [SC21 N 7420]
ISO 8823 DAM 3	Amendment 3: Transfer Syntax Registration, January 1993 [SC21 N 7557]
ISO 8823 AM 4	Amendment 4: Support of Session Symmetric Synchronization Service, November 1993
ISO 8823 AM 5	Amendment 5: Additional Synchronization Functionality to the Presentation Service User, December 1992 [SC21 N 7263]
DIS 8823-1	Information Processing Systems - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Edition 2 of ISO 8823 [SC21 N 8174] (IS expected in 1994) (X.226)
ISO/IEC 8823-2◆	Information Technology - Open Systems Interconnection - Connection Oriented Presentation Protocol Specification, Part 2: Presentation Protocol Implementation Conformance Statement (PICS) Proforma, 1993 (initiation of ITU-TS approval ballot expected February 1994) (X.246)
ISO/IEC 8824◆	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), April 1990, Edition 2 (incorporates AD 1) [SC21 N 4720] (X.208)
ISO/IEC 8824/Cor 1	Draft Technical Corrigendum 1, November 1993 [SC21 N 8317]
ISO/IEC 8824 DAM 2	Amendments to ISO 8824 to Give ISO 8824 Part 1: Specification of Basic Notation, August 1992 [SC21 N 7308] (result is 8824-1; see below)
ISO/IEC 8824 PDAM 3.2	Amendment 3: Rules of Extensibility, 14 August 1992 [SC21 N 6981]

ISO/IEC 8824-1	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), Part 1: Specification of Basic Notation (Edition 3 of ISO 8824), October 1992 (initiation of ITU-TS approval ballot expected February 1994) (X.680)
ISO/IEC 8824-1 WDAM 4	Amendment 4: Removal of Definition of Root Arcs of Object Identifier Tree (WDAM expected August 1994, PDAM December 1994, DAM December 1995, and AM December 1996)
ISO/IEC 8824-2	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), Part 2: Information Object Specification, October 1992 (initiation of ITU-TS approval ballot expected February 1994) (X.681)
ISO/IEC 8824-3	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), Part 3: Constraint Specification, October 1992 (initiation of ITU-TS approval ballot expected February 1994) (X.682)
ISO/IEC 8824-4	Information Technology - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1), Part 4: Parameterization of ASN.1 Specifications, October 1992 (initiation of ITU-TS approval ballot expected February 1994) (X.683)
ISO/IEC 8825♦	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Edition 2 (incorporates AD 1), April 1990 (X.209)
ISO/IEC 8825/Cor 1	Draft Technical Corrigendum 1, November 1993 [SC21 N 8317]
ISO/IEC 8825 DAM 2	Amendments to ISO 8825 to Give ISO 8825 Part 1: Basic Encoding Rules, 19 August 1992 [SC21 N 7312]
ISO/IEC 8825 AM 3	Amendment 3: Rules for Extensibility, June 1992 [SC21 N 6981]
DIS 8825-1	Information Technology - Open Systems Interconnection - Specification of Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 1: Basic Encoding Rules (BER) (revised edition of ISO 8825) (X.690) (IS expected February 1994) (X.690)
DIS 8825-1 WDAM 1	Amendment 1: Light Weight Encoding Rules for ASN.1, August 1993 [SC21 N 7920]
DIS 8825-2.2	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 2: Packed Encoding Rules (PER), 1993 [SC21 N 7302] (initiation of ITU-TS approval ballot expected June 1995) (X.691)
DIS 8825-3	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 3: Distinguished and Canonical Encoding Rules (X.692) (To be merged into text of DIS 8825-1), October 1992 [SC21 N 7313]
DIS 8825-4	Information Technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), Part 4: Test Suite Structure and Test Purposes for ASN.1 Encodings, SC21/WG6, July 1990 [SC21 N 5019]
ISO/IEC 8831	Information Processing Systems - Open Systems Interconnection - Job Transfer and Manipulation (JTM) Concepts and Service, Edition 2, March 1992
ISO/IEC 8832	Information Processing Systems - Open Systems Interconnection - Specification of the Basic Class Protocol for Job Transfer and Manipulation (JTM), Edition 2, March 1992
ISO 8859-1	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 1: Latin Alphabet No. 1, February 1987 (ANSI/ISO 8859-1-1987)
ISO 8859-2	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 2: Latin Alphabet No. 2, February 1987
ISO 8859-3	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 3: Latin Alphabet No. 3, April 1988
ISO 8859-4	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 4: Latin Alphabet No. 4, April 1988
ISO/IEC 8859-5	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 5: Latin/Cyrillic Alphabet, 1988
ISO 8859-6	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 6: Latin/Arabic Alphabet, August 1987
ISO 8859-7	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 7: Latin/Greek Alphabet, November 1987
ISO 8859-8	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 8: Latin/Hebrew Alphabet, 1988
ISO/IEC 8859-9	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 9: Latin Alphabet No. 5, 1989
ISO/IEC 8859-10	Information Processing - 8-Bit Single-Byte Coded Graphic Character Sets, Part 10: Latin Alphabet No. 6, 1992
ISO/IEC 8877♦	Information Technology - Telecommunications and Information Exchange Between Systems - Interface Connector and Contact Assignments for ISDN Basic Access Interface Located at Reference Points S and T, 1992
ISO/IEC 8877 AM 1	Amendment 1: Standard ISDN Basic Access TE Connecting Cord, May 1993
ISO/IEC 8878♦	Information Technology - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Edition 2, 1992 (X.223)
ISO/IEC 8878-2	Information Processing Systems - Data Communications - Use of X.25 to Provide the OSI Connection-Mode Network Service (CONS), Part 2: Protocol Implementation Conformance Statement (PICS), 1992

ISO/IEC 8880-1•	Information Technology - Telecommunications and Information Exchange Between Systems - Protocol Combination to Provide and Support the OSI Network Service, Part 1: General Principles, 1992
ISO/IEC 8880-2•	Information Technology - Telecommunications and Information Exchange Between Systems - Protocol Combination to Provide and Support the OSI Network Service, Part 2: Provision and Support of the Connection-Mode Network Services, 1990
ISO/IEC 8880-2 DAM 1	Amendment 1: Addition of the ISDN Environment (awaiting DAM ballot)
ISO/IEC 8880-2 PDAM 2	Amendment 2: Addition of the PSTN and CSDN Environments (awaiting PDAM ballot)
ISO/IEC 8880-3•	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service, Part 3: Provision and Support of the Connectionless-Mode Network Service, 1990
ISO/IEC 8880-4•	Information Processing Systems - Protocol Combination to Provide and Support the OSI Network Service, Part 4: Interconnection of OSI Environments, 1993
ISO/IEC 8881•	Information Processing Systems - Data Communications - Use of the X.25 Packet Level Protocol (PLP) in Local Area Networks, 1993
ISO 8882	Information Processing Systems - X.25-DTE Conformance Testing, Part 1: General Principles, 1989
ISO/IEC 8882-1	Information Processing Systems - X.25-DTE Conformance Testing, Part 1: General Principles, Edition 2 of ISO 8882, 1993
ISO/IEC 8882-2	Information Technology - Telecommunications and Information Exchange Between Systems - X.25-DTE Conformance Testing, Part 2: Data Link Layer Conformance Test Suite, 1992
ISO/IEC 8882-3	Information Technology - Telecommunications and Information Exchange Between Systems - X.25-DTE Conformance Testing, Part 3: Packet Level Conformance Suite, Edition 3, May 1991
DIS 8883	Information Processing Systems - Text Communication - Message Oriented Text Interchange System, Message Transfer Sublayer, Message Interchange Service and Message Transfer Protocol, February 1986 [WITHDRAWN, superseded by ISO 10021-6]
ISO 8884	Information Processing - Text and Office Systems - Keyboards for Multiple Latin-Alphabet Languages - Layout and Operation Using Four Levels, 1989
ISO 8885:1987•	Information Processing Systems - Data Communication - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format, Edition 1, 1987
ISO/IEC 8885	Information Technology - Telecommunications and Information Exchange Between Systems - High-Level Data Link Control (HDLC) Procedures - General Purpose XID Frame Information Field Content and Format, Edition 2, 1991
ISO/IEC 8885 AM 3	Amendment 3: Definition of a Private Parameter Negotiation Data Link Layer Subfield, August 1992
ISO/IEC 8885 AM 4	Amendment 4: Extended Transparency Options for Start/Stop Transmission, 1992
ISO/IEC 8885 AM 5	Amendment 5: Multi-Selective Reject Option, January 1991
ISO/IEC 8885 PDAM 6	Amendment 6: Seven-bit Transparency Option for Start/Stop Transmission, 1991)
ISO/IEC 8885 PDAM 7	Amendment 7: Frame Check Sequence Negotiation Using the Parameter Negotiation Subfield (ballot closed 21 August 1990)
ISO/IEC 8886•	Information Technology - Telecommunications and Information Exchange Between Systems - Data Link Service Definition for Open Systems Interconnection, Third Revision, 1992
ISO 8907	Information Processing Systems - Database Languages - NDL, June 1987
ISO 9000	Quality Management and Quality Assurance Standards - Guidelines for Selection and Use, 1987
ISO 9000-3	Quality Management and Quality Assurance Standards, Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply, and Maintenance of Software, 1991
ISO 9001	Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation and Servicing, 1987
ISO 9002	Quality Systems - Model for Quality Assurance in Production and Installation, 1987
ISO 9003	Quality Systems - Model for Quality Assurance in Final Inspection and Test, 1987
ISO 9004	Quality Management and Quality System Elements - Guidelines, 1987
ISO 9004-2	Quality Management and Quality System Elements, Part 2: Guidelines for Services, 1991
ISO/TR 9007	Information Processing Systems - Concepts and Terminology for the Conceptual Schema and the Information Base, July 1987
ISO 9036	Information Processing - Arabic 7-bit Coded Character Set for Information Exchange, 1987
ISO 9040•	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Service - Base Class, Revised Edition (incorporates AD 1), November 1990
ISO 9040/Cor 1	Technical Corrigendum 1, April 1991
ISO 9040/Cor 2	Technical Corrigendum 2, December 1992
ISO 9040/Cor 3	Technical Corrigendum 3, September 1993
ISO 9040 AM 2•	Amendment 2: Additional Functional Units, October 1992 [SC21 N 7878]
ISO 9041-1:1990•	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Protocol, Part 1: Specification, Revised Edition of ISO 9041 (incorporates AD 1), November 1990
ISO 9041-1/Cor 1	Technical Corrigendum 1, December 1992
ISO 9041-1/Cor 2	Technical Corrigendum 1, September 1993
ISO 9041-1 AM 2•	Amendment 2: Additional Functional Units, October 1992

ISO 9041-2◆	Information Processing Systems - Open Systems Interconnection - Virtual Terminal (VT) Protocol, Part 2: VT PICS Proforma, 1993 (DIS ballot ended October 1991)
DIS 9065	Information Processing Systems - Text Communication - Message Oriented Text Interchange System (MOTIS) User Agent Sublayer - Interpersonal Messaging User Agent - Message Interchange Formats and Protocols, February 1986 [withdrawn; superseded by ISO 10021]
ISO/IEC 9066-1◆	Information Processing Systems - Text Communication - Reliable Transfer (RT), Part 1: Model and Service Definition, Revised Edition, September 1989 [SC21 N 3883] (X.218)
ISO/IEC 9066-2◆	Information Processing Systems - Text Communication - Reliable Transfer (RT), Part 2: Protocol Specification, Revised Edition, September 1989 [SC21 N 3884] (X.228)
ISO/IEC 9066-2/Cor 1	Technical Corrigendum 1, September 1993 [SC21 N 8077]
DIS 9066-3	Information Processing Systems - Text Communication - Reliable Transfer (RT), Part 3: PICS Proforma, March 1993 [SC21 N 7677] (initiation of ITU-TS approval ballot expected June 1995) (X.248)
ISO 9067	Information Processing Systems - Data Communication - Automatic Fault Isolation Procedures Using Test Loops, September 1987
DIS 9068◆	Information Processing Systems - Provision of the Connectionless Network Service (CONS) Using ISO 8208, 1989
ISO 9069	Information Processing - SGML Support Facilities - SGML Document Interchange Format (SDIF), September 1988
ISO/IEC 9070	Information Processing - SGML Support Facilities - Registration Procedures for Public Text Owner Identifiers, Edition 2, April 1991
DP 9071-1.2	Text and Office Systems - Basic and Optional Requirements, Part 1: Facsimile Equipment, Revision 2, January 1987
DP 9071-2.2	Text and Office Systems - Basic and Optional Requirements, Part 2: Text Communications Terminals, Revision 2, January 1987
ISO 9072-1:1989◆	Information Processing Systems - Text Communication - Remote Operations, Part 1: Model, Notation and Service Definition, Revised Edition, September 1989 [SC21 N 3881] (X.219)
ISO 9072-1 PDAM 1	Amendment 1: Enhancements to Service Definition, April 1992 [SC21 N 6717] (to JTC1 for endorsement to cancel the project)
ISO/IEC 9072-1:1993	Information Processing Systems - Text Communication - Remote Operations, Part 1: Concepts, Model and Notation, Edition 2, March 1993 [SC21 N 7669] (passed DIS ballot in October 1993) (X.219) (see DIS 13712-1)
ISO/IEC 9072-1 PDAM 1	Amendment 1: Built-In Operations, June 1993 [SC21 N 8073]
ISO/IEC 9072-2:1989◆	Information Processing Systems - Text Communication - Remote Operations, Part 2: Protocol Specification, Revised Edition, September 1989 [SC21 N 3882] (X.229)
ISO/IEC 9072-2 PDAM 1	Amendment 1: Enhancements to Protocol Specification, April 1992 [SC21 N 6718] (to JTC1 for endorsement to cancel the project)
ISO/IEC 9072-2:1993	Information Processing Systems - Text Communication - Remote Operations, Part 2: Service Definition, Edition 2, March 1993 (passed DIS ballot in October 1993) [SC21 N 7670] (see DIS 13712-2)
ISO/IEC 9072-2 PDAM 1	Amendment 1: Mapping to A-UNITDATA and Built-In Operations, July 1993 [SC21 N 8074]
ISO/IEC 9072-3:1993	Information Processing Systems - Text Communication - Remote Operations, Part 3: Protocol Specification, March 1993 (passed DIS ballot in October 1993) [SC21 N 8074] (see DIS 13712-3)
ISO/IEC 9072-3 PDAM 1	Amendment 1: Mapping to A-UNITDATA and Built-In Operations, June 1993 [SC21 N 8075]
DIS 9072-4	Information Processing Systems - Text Communication - Remote Operations, Part 4: PICS Proforma, December 1993 [SC21 N 7678] (initiation of ITU-TS approval ballot expected November 1994) (X.249) (see CD 13712-4)
ISO 9074:1989	Information Processing Systems - Open Systems Interconnection - Estelle - A Formal Description Technique Based on an Extended State Transition Model, July 1989
ISO 9074 AM 1	Amendment 1: Estelle Tutorial, 1993
WD 9074.2	Information Technology - Open Systems Interconnection - Estelle - A Formal Description Technique Based on an Extended State Transition Model, Edition 2 (incorporates AM 1)
ISO 9075:1988	Information Processing Systems - Database Language SQL, April 1989 (revised text incorporates AD 1) [SC21 N 3158]
ISO 9075:1992	Information Technology - Database Languages - SQL2, November 1992 (technical content of ISO 9075:1988 is retained as a level of the 1992 standard)
ISO 9075:1992/Cor 1	Technical Corrigendum 1, January 1994 [SC21 N 8432]
WD 9075-x	Information Processing Systems - Database Languages - SQL, Part x: SQL Call Level Interface (CLI), January 1993 [SC21 N 7596] (CD expected January 1994)
WD 9075-y	Information Processing Systems - Database Languages - SQL, Part y: Persistent SQL Modules, January 1993 [SC21 N 7597] (CD expected January 1994)
WD 9075.3	Information Processing Systems - Database Languages - SQL3, May 1992 [SC21 N 6931 and SC21 N 8091] (CD text expected July 1994; DIS July 1995; IS July 1996)
ISO/IEC 9126	Information Technology - Software Product Evaluation - Quality Characteristics and Guidelines for Their Use, 1991

ISO 9127	Information Processing Systems - User Documentation and Cover Information for Consumer Software Packages, 1988
ISO 9160	Information Processing - Data Encipherment - Physical Layer Interoperability Requirements, February 1988
ISO 9171-1	Information Technology - 130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 1: Unrecorded Optical Disk Cartridge, 1990
ISO 9171-2	Information Technology - 130 mm Optical Disk Cartridge, Write Once, for Information Interchange, Part 2: Recording Format, 1990
DIS 9234	Industrial Asynchronous Data Link for Two-Way Simultaneous or Two-Way Alternate Mode, 1989
ISO 9241-1	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 1: Introduction, 1992
ISO 9241-2	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 2: General Guidance on Task Requirements, 1992
ISO 9241-3	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 3: Visual Display Requirements, 1992
DIS 9241-4	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 4: Keyboard Requirements
CD 9241-5	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 5: Workstation Layout and Postural Requirements
CD 9241-6	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 6: Environmental Requirements
CD 9241-7	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 7: Display Requirements with Reflections
CD 9241-8	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 8: Requirements for Displayed Colors
CD 9241-9	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 9: Requirements for Non-Keyboard Input Devices
WD 9241-10	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 10: Dialogue Principles
CD 9241-11	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 11: Usability Statements
CD 9241-12	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 12: Presentation of Information
WD 9241-13	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 13: User Guidance
CD 9241-14	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 14: Menu Dialogues
WD 9241-15	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 15: Command Dialogues
WD 9241-16	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 16: Direct Manipulation Dialogues
WD 9241-17	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 17: Form-Filling Dialogues
XX 9241-18	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 18: Question and Answer Dialogues (not yet started)
XX 9241-19	Ergonomic Requirements for Office Work with Visual Display Terminals, Part 19: Natural Language Dialogues (not yet started)
ISO 9281-1	Information Technology - Identification of Picture Coding Methods, Part 1: Identification, August 1990
ISO 9281-2	Information Technology - Identification of Picture Coding Methods, Part 2: Procedure for Registration, August 1990
ISO 9282-1	Information Technology - Coded Representation of Pictures, Part 1: Encoding Principles for Picture Representation in a 7- or 8-Bit Environment, September 1988
ISO 9282-2	Information Technology - Coded Representation of Pictures, Part 2: Encoding Principles for Photographic Images, May 1992
ISO/IEC TR 9294	Information Technology - Guidelines for the Management of Software Documentation, Technical Report Type 3, 1990
ISO 9314-1♦	Information Processing Systems- Fiber Distributed Data Interface (FDDI), Part 1: Token Ring Physical Layer Protocol (PHY), 1989
ISO 9314-2♦	Information Processing Systems- Fiber Distributed Data Interface (FDDI), Part 2: Token Ring Media Access Control (MAC), 1989
ISO/IEC 9314-3♦	Information Technology- Fiber Distributed Data Interface (FDDI), Part 3: Physical Layer Medium Dependent (PMD), August 1990
ISO/IEC 9314-4♦	Information Technology - Fiber Distributed Data Interface (FDDI), Part 4: Single Mode Fiber/Physical Layer Medium Dependent Physical Connectors (SMF-PMD), 1993
DIS 9314-5♦	Information Technology - Fiber Distributed Data Interface (FDDI), Part 5: Hybrid Ring Control (HRC), 1993

CD 9314-6	Information Technology - Fiber Distributed Data Interface (FDDI), Part 6: Station Management (SMT) Standard, 1993
ISO 9316	Information Processing Systems - Small Computer System Interface (SCSI), 1989
DIS 9318-1	Information Processing Systems - Intelligent Peripheral Interface, Part 1: Physical Level, August 1987
ISO 9318-2	Information Processing Systems - Intelligent Peripheral Interface, Part 2: Device Specific Command Set for Magnetic Disk Drives, 1990 (ANSI/ISO 9318-2-1990)
ISO 9318-3	Information Processing Systems - Intelligent Peripheral Interface, Part 3: Device Generic Command Set for Magnetic and Optical Disk Drives, 1990 (ANSI/ISO 9318-3-1990)
ISO 9318-4	Information Processing Systems - Intelligent Peripheral Interface, Part 4: Device Generic Command Set for Magnetic Tape Drives, 1990 (ANSI/ISO 9318-4-1990)
DIS 9324	Information Processing - Storage Module Interfaces, September 1988
ISO 9496	Information Processing - Programming Languages - CCITT High Level Language (CHILL), August 1989 (Z.200)
ISO 9506-1	Industrial Automation Systems - Manufacturing Message Specification, Part 1: Service Definition, 1990
ISO 9506-1 AD 1	Amendment 1: Data Exchange, 1993
ISO 9506-2	Industrial Automation Systems - Manufacturing Message Specification, Part 2: Protocol Specification, 1990
ISO 9506-2 AD 1	Amendment 1: Data Exchange, 1993
ISO 9506-3	Industrial Automation Systems - Manufacturing Message Specification, Part 3: Companion Standard for Robotics, 1991
ISO 9506-4	Industrial Automation Systems - Manufacturing Message Specification, Part 4: Companion Standard for Numerical Control, 1992
ISO/IEC 9541-1	Information Technology - Font Information Exchange, Part 1: Architecture, May 1991
ISO/IEC 9541-1/Cor 1	Technical Corrigendum 1, 1992
ISO/IEC 9541-2	Information Technology - Font Information Exchange, Part 2: Interchange Format, May 1991
DIS 9541-3	Information Technology - Font and Character Information Exchange, Part 3: Character Identification Method, October 1991
DIS 9541-4	Information Processing Systems- Font and Character Information Exchange, Part 4: Character Collections, December 1987
DIS 9541-5	Information Processing Systems- Font and Character Information Exchange, Part 5: Font Attributes and Character Model, December 1987
DIS 9541-6	Information Processing Systems- Font and Character Information Exchange, Part 6: Font and Character Attribute Subsets and Application, December 1987
DP 9541-7	Information Processing Systems- Font and Character Information Exchange, Part 7: Font Interchange Format, May 1987
ISO 9542•	Information Processing Systems- Telecommunications and Information Exchange Between Systems - End System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-Mode Network Service (ISO 8473), 1988 (Revised Edition, 1989)
ISO 9542 PDAM 1	Amendment 1: Dynamic Discovery of OSI NSAP Addresses by End Systems (New Work Item)
ISO 9543•	Information Processing Systems - Information Exchange Between Systems - Synchronous Transmission Signal Quality at DTE/DCE Interfaces, May 1989
ISO/TR 9544	Information Processing - Computer-Assisted Publishing - Vocabulary, December 1988
ISO/IEC 9545•	Information Technology - Open Systems Interconnection - Application Layer Structure (ALS), Edition 2 (incorporates AM 1 and AM 2), December 1993
ISO/TR 9547	Programming Language Processors - Test Methods - Guidelines for Their Development and Acceptability, April 1988
ISO 9548•	Information Technology - Open Systems Interconnection - Session Connectionless Protocol to Provide the Connectionless-Mode Session Service, August 1989 (held pending publication of ISO 8326 and 8327:1) (X.235)
ISO/IEC 9548-2	Information Technology - Open Systems Interconnection - Session Connectionless Protocol to Provide the Connectionless-Mode Session Service, Part 2: PICS Proforma, April 1993 [SC21 N 7679] (approved for IS in October 1993; initiation of ITU-TS approval ballot expected February 1994) (X.255)
ISO 9549•	Information Technology - Galvanic Isolation of Balanced Interchange Circuit, October 1990
ISO 9564-1	Financial Transactions - Retail Banking Security - Personal Identification Number (PIN) Management and Security, Part 1: PIN Protection Principles and Techniques, TC68/SC6/WG6
ISO 9564-2	Financial Transactions - Retail Banking Security - Personal Identification Number (PIN) Management and Security, Part 2: Approved Algorithms for PIN Encipherment, TC68/SC6/WG6
ISO/IEC TR 9571•	Information Technology - Open Systems Interconnection - LOTOS Description of the Session Service, September 1989 (TR has been cancelled now that the Edition 2 of Session Service has been published)

ISO/IEC TR 9572◆	Information Technology - Open Systems Interconnection - LOTOS Description of the Session Protocol, September 1989 (TR has been cancelled now that the Edition 2 of Session Service has been published)
WDTR 9573-1	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 1: SGML Tutorial, December 1988
WDTR 9573-2	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 2: Basic Technique, December 1988
WDTR 9573-3	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 3: Advanced Techniques - Using LINK and CONCUR, December 1988
WDTR 9573-4	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 4: Advanced Techniques - Using SHORTREF to Indicate Markup, December 1988
WDTR 9573-5	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 5: Using Non-Latin Alphabets, December 1988
WDTR 9573-6	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 6: Referencing and Synchronization, December 1988
WDTR 9573-7	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 7: Mathematics and Chemistry, December 1988
WDTR 9573-8	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 8: Tables, December 1988
WDTR 9573-9	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 9: Using SGML for Computer to Computer Interchange, December 1988
WDTR 9573-10	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 10: Designing Applications for Database Interfacing, December 1988
ISO/IEC TR 9573-11	Information Technology - SGML Support Facilities - Techniques for Using SGML, Part 11: Application at ISO Central Secretariat for International Standards and Technical Reports, 1992
ISO/IEC TR 9573-12	Information Technology - SGML Support Facilities - Techniques for Using SGML, Part 12: Public Entity Sets for General and Publishing Symbols, 1991
ISO/IEC TR 9573-13	Information Technology - SGML Support Facilities - Techniques for Using SGML, Part 13: Public Entity Sets for Mathematics and Science, June 1991
WDTR 9573-14	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 14: Public Entity Sets for Latin Based Alphabets, December 1988
WDTR 9573-15	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 15: Public Entity Sets for Non-Latin Based Alphabets, December 1988
WDTR 9573-16	Information Processing - SGML Support Facilities - Techniques for Using SGML, Part 16: Public Entity Sets for Ideograms, December 1988
ISO/IEC 9574◆	Information Technology - Provision of the OSI Connection-Mode Network Service (CONS) by Packet Mode Terminal Equipment Connected to an Integrated Services Digital Network (ISDN), Edition 2, 1992
ISO/IEC 9574 DAM 1	Amendment 1: Provision of the CONS on an ISDN Circuit-Switch Channel Connecting Directly to the Remote Terminal, April 1991
ISO/IEC TR 9575◆	Information Technology - Telecommunications and Information Exchange Between Systems - OSI Routing Framework, June 1990
ISO/IEC 9576◆	Information Technology - Open Systems Interconnection - Connectionless Presentation Protocol Specification, 1991 (X.236)
DIS 9576-2◆	Information Technology - Open Systems Interconnection - Presentation Protocol to Provide the Connectionless-Mode Presentation Service, Part 2: PICS Proforma for Connectionless Presentation Protocol, July 1991 [SC21 N 5930] (IS text expected March 1994) (X.256)
ISO/IEC TR 9577◆	Protocol Identification in the OSI Network Layer, 1993
ISO/IEC TR 9578	Communication Interface Connectors Used in Local Area Networks, May 1990
ISO 9579-1◆	Information Technology - Database Languages - Remote Database Access (RDA) - Part 1: Generic Model, Service and Protocol, March 1993 [SC21 N 7689]
ISO 9579-1 WDAM 1	Amendment 1: Generic RDA, August 1992 [SC21 N 7202] (PDAM expected July 1994; DAM July 1995; AM July 1996])
ISO 9579-2◆	Information Technology - Database Languages - Remote Database Access (RDA) - Part 2: SQL Specialization, March 1993 [SC21 N 7703)
ISO 9579-2 PDAM 1	Amendment 1: Support for SQL 1992, September 1993 [SC21 N 8307]
ISO 9579-2 WDAM 2	Amendment 2: RDA Support for Stored DBL Statements, October 1990 [SC21 N 5138] (rapporteur meeting January 1994; PDAM expected July 1995)
CD 9579-3	Information Technology - Database Languages - Remote Database Access (RDA) - Part 3: SQL PICS Proforma, October 1993 [SC21 N 8087] (editing meeting January 1994)
ISO 9592-1	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS), Part 1: Functional Description, May 1989 (ANSI/ISO 9592-1-1989)
ISO 9592-1 AM 1	Amendment 1: PHIGS Plus Support, 1992 (ANSI/ISO 9592-1a-1992)
ISO 9592-2	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS), Part 2: Archive File Format, May 1989 (ANSI/ISO 9592-2-1989)

ISO 9592-2 AM 1	Amendment 1: PHIGS Plus Support, September 1992 (ANSI/ISO 9592-2a-1992)
ISO 9592-3	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS), Part 3: Clear-Text Encoding of Archive File, May 1989 (ANSI/ISO 9592-3-1989)
ISO 9592-4	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS), Part 4: Plus Lumiere und Surfaces (PHIGS Plus), 1992 (ANSI/ISO 9592-4-1992)
ISO/IEC 9593-1	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings, Part 1: FORTRAN, August 1990 (ANSI/ISO 9593.1-1992)
DIS 9593-2	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings, Part 2: Extended Pascal (awaiting DIS ballot)
ISO/IEC 9593-3	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings, Part 3: Ada, July 1990 (ANSI/ISO 9593.3-1990)
ISO/IEC 9593-3 DAM 1	Amendment 1: Incorporation of PHIGS Plus
ISO/IEC 9593-4	Information Technology - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Language Bindings, Part 4: C, 1991 (ANSI/ISO 9593.4-1991)
ISO/IEC 9594-1♦	Information Technology - Open Systems Interconnection - The Directory, Part 1: Overview of Concepts, Models and Services, December 1990 (X.500:1988)
ISO/IEC 9594-1 AM 1♦	Amendment 1: Replication, Schema and Access Control, January 1992 [SC21 N 6502] (successfully passed ballot September 1992)
ISO/IEC 9594-1/9 WDAMs	Amendments to Parts 1 to 9 on Internationalization of the Directory Enhancement of Directory, 1993 (NWI proposal) [JTC1 N 2039]
ISO/IEC 9594-1/9 WDAMs	Amendments to Parts 1 to 9 on Enhancement of Directory Operational Security, 1993 (NWI proposal) [JTC1 N 2248]
ISO/IEC 9594-1/9 WDAMs	Amendments to Parts 1 to 9 on Directory Schema Migration, 1993 (NWI proposal) [SC21 N 7942]
DIS 9594-1.2	Information Technology - Open Systems Interconnection - The Directory, Part 1: Overview of Concepts, Models and Services, Edition 2 (incorporates AM1), 1993 (ITU-TS ballot closed November 1993) (X.500:1993)
ISO/IEC 9594-2♦	Information Technology - Open Systems Interconnection - The Directory, Part 2: Models, December 1990 (X.501:1988)
ISO/IEC 9594-2/Cor 1	Technical Corrigendum 1, 1991
ISO/IEC 9594-2/Cor 2	Technical Corrigendum 2, July 1992
ISO/IEC 9594-2 AM 1♦	Amendment 1: Access Control, January 1992 [SC21 N 6502] (successfully passed ballot September 1992)
ISO/IEC 9594-2 AM 2	Amendment 2: Schema Extensions, January 1992 [SC21 N 6503] (successfully passed ballot September 1992)
ISO/IEC 9594-2 AM 3	Amendment 3: Replication, January 1992 [SC21 N 6504] (successfully passed ballot September 1992)
DIS 9594-2.2	Information Technology - Open Systems Interconnection - The Directory, Part 2: Models, Edition 2 (incorporates AM1, AM2, and AM3), 1993 (ITU-TS ballot closed November 1993) (X.501:1993)
ISO/IEC 9594-3♦	Information Technology - Open Systems Interconnection - The Directory, Part 3: Abstract Service Definition, December 1990 (X.511:1988)
ISO/IEC 9594-3/Cor 1	Technical Corrigendum 1, December 1991
ISO/IEC 9594-3/Cor 2	Technical Corrigendum 2, July 1992
ISO/IEC 9594-3/Cor 3	Technical Corrigendum 3, October 1992
ISO/IEC 9594-3/Cor 4	Technical Corrigendum 4, March 1993
ISO/IEC 9594-3 AM 1♦	Amendment 1: Access Control, January 1992 [SC21 N 6505] (successfully passed ballot September 1992)
ISO/IEC 9594-3 AM 2	Amendment 2: Replication, Schema and Enhanced Search, January 1992 [SC21 N 6506] (successfully passed ballot in September 1992)
DIS 9594-3.2	Information Technology - Open Systems Interconnection - The Directory, Part 3: Abstract Service Definition, Edition 2 (incorporates AM1 and Am2), 1993 (ITU-TS ballot closed November 1993) (X.511:1993)
ISO/IEC 9594-4♦	Information Technology - Open Systems Interconnection - The Directory, Part 4: Procedures for Distributed Operations, December 1990 (X.518:1988)
ISO/IEC 9594-4/Cor 1	Technical Corrigendum 1, December 1991
ISO/IEC 9594-4/Cor 2	Technical Corrigendum 2, July 1992
ISO/IEC 9594-4/Cor 3	Technical Corrigendum 3, March 1993
ISO/IEC 9594-4 AM 1♦	Amendment 1: Access Control, January 1992 [SC21 N 6507] (successfully passed ballot September 1992)
ISO/IEC 9594-4 AM 2	Amendment 2: Replication, Schema and Enhanced Search, January 1992 [SC21 N 6508] (successfully passed ballot in September 1992)
DIS 9594-4.2	Information Technology - Open Systems Interconnection - The Directory, Part 4: Procedures for Distributed Operations, Edition 2 (incorporates AM1 and AM2), 1993 (ITU-TS ballot closed November 1993) (X.518:1993)

ISO/IEC 9594-5◆	Information Technology - Open Systems Interconnection - The Directory, Part 5: Protocol Specifications, December 1990 (X.519:1988)
ISO/IEC 9594-5/Cor 1	Technical Corrigendum 1, October 1992
ISO/IEC 9594-5 AM 1◆	Amendment 1: Replication, 2 January 1992 [SC21 N 6509] (approved 5 September 1992)
DIS 9594-5.2	Information Technology - Open Systems Interconnection - The Directory, Part 5: Protocol Specifications, Edition 2 (incorporates AM1), 1993 (ITU-TS ballot closed November 1993) (X.519:1993)
ISO/IEC 9594-6◆	Information Technology - Open Systems Interconnection - The Directory, Part 6: Selected Attribute Types, December 1990 (X.520:1988)
ISO/IEC 9594-6 AM 1◆	Amendment 1: Schema Extensions, 2 January 1992 [SC21 N 6510] (approved 5 September 1992)
DIS 9594-6.2	Information Technology - Open Systems Interconnection - The Directory, Part 6: Selected Attribute Types, Edition 2 (incorporates AM1), 1993 (ITU-TS ballot closed November 1993) (X.520:1993)
ISO/IEC 9594-7◆	Information Technology - Open Systems Interconnection - The Directory, Part 7: Selected Object Classes, December 1990 (X.521:1988)
ISO/IEC 9594-7/Cor 1	Technical Corrigendum 1, December 1991
ISO/IEC 9594-7/Cor 2	Technical Corrigendum 2, July 1992
ISO/IEC 9594-7 AM 1◆	Amendment 1: Schema Extensions, 2 January 1992 [SC21 N 6511] (approved 5 September 1992)
DIS 9594-7.2	Information Technology - Open Systems Interconnection - The Directory, Part 7: Selected Object Classes, Edition 2 (incorporates AM1), 1993 (ITU-TS ballot closed November 1993) (X.521:1993)
ISO/IEC 9594-8◆	Information Technology - Open Systems Interconnection - The Directory, Part 8: Authentication Framework, December 1990 (X.509)
ISO/IEC 9594-8/Cor 1	Technical Corrigendum 1, 1991
ISO/IEC 9594-8 AM 1◆	Amendment 1: Access Control, 2 January 1992 [SC21 N 6512] (approved 5 September 1992)
ISO/IEC 9594-8 WDAM	Amendment on Security Enhancement to Directory (Extensions for Certificate Definitions) (NWI proposal accepted April 1993; PDAM expected July 1995)
DIS 9594-8.2	Information Technology - Open Systems Interconnection - The Directory, Part 8: Authentication Framework, Edition 2 (incorporates AM1), 1993 (ITU-TS ballot closed November 1993) (X.509:1993)
ISO/IEC 9594-9◆	Information Technology - Open Systems Interconnection - The Directory, Part 9: Replication, January 1992 [SC21 N 6513] (ITU-TS ballot closed November 1993) (X.525:1993)
CD 9594-10◆	Information Technology - Open Systems Interconnection - The Directory, Part 10: PICS Proforma, for the OSI Directory DUA Protocol, 1993 (fast-track ballot requested) (X.581:1992)
WD 9594-11	Information Technology - Open Systems Interconnection - The Directory, Part 11: PICS Proforma, for the OSI Directory DSA Protocol, 1993 (fast-track ballot requested) (X.582:1992)
WD 9594-w	Information Technology - Open Systems Interconnection - The Directory, Part x: Use of Systems Management for Administration of the Directory, June 1993 [SC21 N 7930] (CD expected July 1994]
ISO/IEC 9595◆	Information Technology - Open Systems Interconnection - Common Management Information Service (CMIS) Definition, Edition 2 (incorporates AD1 and AD 2), April 1991 (X.710:1991)
ISO/IEC 9595/Cor 1	Technical Corrigendum 1, April 1992 [SC21 N 8166]
ISO/IEC 9595/Cor 2	Technical Corrigendum 2, July 1992
ISO/IEC 9595 PDAM 3	Amendment 3: Support of Allomorphism, 26 November 1990 [SC21 N 4966] (SC21 has asked JTC1 for endorsement to cancel this project)
ISO/IEC 9595 AM 4	Amendment 4: Access Control, July 1992
ISO/IEC 9595 WDAM 5	Amendment 5: Enhanced Functionality for System Management Communications, June 1993 (expected to become Edition 3 of ISO 9595; PDAM expected December 1994)
ISO/IEC 9596-1◆	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP), Part 1: Specification, Edition 2 (incorporates AD1 and AD 2 of ISO 9596:1990), April 1991 (X.711:1991)
ISO/IEC 9596-1/Cor 1	Technical Corrigendum 1, April 1992
ISO/IEC 9596-1/Cor 2	Technical Corrigendum 2, July 1992
ISO/IEC 9596-1/Cor 3	Technical Corrigendum 3, September 1992
ISO/IEC 9596-1/Cor 4	Technical Corrigendum 3, March 1993
ISO/IEC 9596 PDAM 3	Amendment 3: Support of Allomorphism, July 1990 [SC21 N 4967] [JTC1 N 761] (SC21 has asked JTC1 for endorsement to cancel this project)
ISO/IEC 9596 PDAM 4	Amendment 4: State Table, January 1990 [SC21 N 4058] (new work item June 1990; terminated June 1991)
ISO/IEC 9596 WDAM 5	Amendment 5: Enhanced Functionality, June 1993 [SC21 N 7970] (PDAM expected December 1994)
ISO/IEC 9596-2◆	Information Technology - Open Systems Interconnection - Common Management Information Protocol (CMIP) Specification, Part 2: PICS Proforma, 21 July 1992 [SC21 N 7111] (X.712)
ISO/IEC 9596-2/Cor 1	Technical Corrigendum 1, June 1993

ISO/IEC 9636-1	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 1: Overview, Profiles, and Conformance, May 1991 (ANSI/ISO 9636-1-1991)
ISO/IEC 9636-2	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 2: Control, Negotiation, and Errors, May 1991 (ANSI/ISO 9636-2-1991)
ISO/IEC 9636-3	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 3: Output and Attributes, May 1991 (ANSI/ISO 9636-3-1991)
ISO/IEC 9636-4	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 4: Segmentation, May 1991 (ANSI/ISO 9636-4-1991)
ISO/IEC 9636-5	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 5: Input and Echoing, May 1991 (ANSI/ISO 9636-5-1991)
ISO/IEC 9636-6	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 6: Raster, May 1991 (ANSI/ISO 9636-6-1991)
WD 9636-8	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 8: FORTRAN Language Binding of CGI, 1989
WD 9636-11	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI), Part 11: C Language Binding of CGI, 1989
DIS 9637-1	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI) - Data Stream Binding, Part 1: Character Encoding (review period ends 19 November 1991)
ISO/IEC 9637-2	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI) - Data Stream Binding, Part 2: Binary Encoding, 1992
DIS 9637-3	Information Technology - Computer Graphics - Interfacing Techniques for Dialogues with Graphical Devices - Functional Specification (CGI) - Data Stream Binding, Part 3: Clear Text Encoding
DIS 9638-1	Interface Techniques for Dialogues with Graphical Devices - CGI Language Bindings, Part 1: FORTRAN
DIS 9638-2	Interface Techniques for Dialogues with Graphical Devices - CGI Language Bindings, Part 2: Pascal
DIS 9638-3	Interface Techniques for Dialogues with Graphical Devices - CGI Language Bindings, Part 3: Ada
DIS 9638-4	Interface Techniques for Dialogues with Graphical Devices - CGI Language Bindings, Part 4: C (review period ends 10 September 1991)
ISO/IEC 9646-1♦	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 1: General Concepts, July 1991 [SC21 N 5865] (X.290)
ISO/IEC 9646-1 Cor 1	Technical Corrigendum 1, October 1993 [SC21 N 8293]
ISO/IEC 9646-1 AM 1	Amendment 1: Protocol Profile and Multi-Protocol Testing, October 1993
ISO/IEC 9646-1 AM 2	Amendment 2: Multi-Party Testing Methodology, October 1993
DIS 9646-1.2	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 1: General Concepts, Edition 2 (incorporates AM1 and AM2) (IS text expected March 1994) (X.290)
ISO/IEC 9646-2♦	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 2: Abstract Test Suite Specification (Excluding Annexes E and F on TTCN), May 1991 [SC21 N 5867] (X.291)
ISO/IEC 9646-2 Annex	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 2: Abstract Test Suite Specification, Annex: Guidelines for PICS Proformas [SC6 N 6243]
ISO/IEC 9646-2 AM 1	Amendment 1: Protocol Profile and Multi-Protocol Testing, October 1993
ISO/IEC 9646-2 AM 2	Amendment 2: Multi-Party Testing Methodology, October 1993
DIS 9646-2.2	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 2: Abstract Test Suite Specification, Edition 2 (X.291)
ISO/IEC 9646-3♦	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 3: The Tree and Tabular Combined Notation (TTCN), October 1992 (X.292)
ISO/IEC 9646-3 AM 1	Addendum 1: TTCN Extensions, October 1993
ISO/IEC 9646-3 DAM 2	Amendment 2: Further TTCN Extensions, December 1993 [SC21 N 8374]
ISO/IEC 9646-4♦	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 4: Test Realization, July 1991 (X.293)
ISO/IEC 9646-4 AM 1	Amendment 1: Protocol Profile and Multi-Protocol Testing, October 1993 [SC21 N 7325]
ISO/IEC 9646-4 AM 2	Amendment 2: Multi-Party Testing Methodology, October 1993 [SC21 N 7326]
DIS 9646-4.2	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 4: Test Realization, Edition 2, 1993 (X.293)
ISO/IEC 9646-5♦	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process, July 1991 (X.294)

ISO/IEC 9646-5 Cor 1	Technical Corrigendum 1, October 1993 [SC21 N 8294]
ISO/IEC 9646-5 AM 1	Amendment 1: Protocol Profile and Multi-Protocol Testing, October 1993
ISO/IEC 9646-5 AM 2	Amendment 2: Multi-Party Testing Methodology, October 1993
DIS 9646-5.2	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 5: Requirements on Test Laboratories and Clients for the Conformance Assessment Process, Edition 2, 1993 (X.294)
ISO/IEC 9646-6	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 6: Protocol Profile Test Specification, 1993 [SC21 N 7329] (editing meeting September 1993; IS text expected March 1994) (X.295)
DIS 9646-7	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework, Part 7: Requirements and Guidelines on Implementation Conformance Statement (ICS) and ICS Proformas, October 1993 [SC21 N 8180] (editing meeting July 1994)
ISO 9660	Information Processing - Volume and File Structure of CD-ROM for Information Exchange, April 1988
ISO 9735	Electronic Data Interchange for Administration, Commerce and Transport (EDIFACT) - Application Level Syntax Rules, July 1988 (amended and reprinted in 1990)
ISO 9735 AM 1	Amendment 1, 1992
TR 9789	Information Technology - Guidelines for the Organization and Representation of Data Elements for Data Interchange - Coding Methods and Principles, November 1993
ISO/IEC 9796	Information Technology - Security Techniques - Digital Signature Scheme Giving Message Recovery, 1991
ISO/IEC 9797	Information Technology - Data Cryptographic Techniques - Data Integrity Mechanism Using a Cryptographic Check Function Employing a Block Cipher Algorithm, 1989
ISO/IEC 9798-1	Information Processing - Security Techniques - Entity Authentication Mechanisms, Part 1: General Model, 1991
DIS 9798-2	Information Technology - Security Techniques - Entity Authentication Mechanisms, Part 2: Entity Authentication Using Symmetric Techniques, SC27/WG2, 1993
DIS 9798-3	Information Technology - Security Techniques - Entity Authentication Mechanisms, Part 3: Entity Authentication Using a Public Key Algorithm, SC27/WG2, 1993
WD 9798-4	Information Technology - Security Techniques - Entity Authentication Mechanisms, Part 4: Entity Authentication Using Non-Reversible Functions, SC27/WG2, 1993
WD 9798-x	Information Technology - Security Techniques - Entity Authentication Mechanisms, Part x: Entity Authentication Using Zero-Knowledge Techniques, SC27/WG2, 1993
ISO/IEC 9804♦	Information Technology - Open Systems Interconnection - Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element, November 1990 (X.851:1993)
ISO/IEC 9804/Cor 1	Technical Corrigendum 1, December 1991
ISO/IEC 9804 PDAM 1.2	Amendment 1: Enhancements, July 1992 [SC21 N 7246] (DIS text expected June 1994 and IS expected June 1995)
ISO/IEC 9804 AM 2	Amendment 2: Session Mapping Changes (Additional Synchronization Functionality), December 1992 [SC21 N 7278]
ISO/IEC 9804 WDAM 3	Amendment 3: Restart (SC21 has asked JTC1 for endorsement to cancel the project))
DIS 9804.2	Information Technology - Open Systems Interconnection - Service Definition for the Commitment, Concurrency, and Recovery (CCR) Service Element, Edition 2 (incorporates AM 1 and AM 2), January 1993 [SC21 N 7659] (ballot closed November 1993)
ISO/IEC 9805♦	Information Technology - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Service, November 1990 (X.247)
ISO/IEC 9805/Cor 1	Technical Corrigendum 1, December 1991
ISO/IEC 9805/Cor 2	Technical Corrigendum 2, December 1992
ISO/IEC 9805 PDAM 1.2	Amendment 1: Enhancements, July 1992 [SC21 N 7247] (DIS text expected June 1994, IS text June 1995)
ISO/IEC 9805 AM 2	Amendment 2: Session Mapping Changes (Additional Synchronization Functionality), December 1992 [SC21 N 7279]
ISO/IEC 9805 WDAM 3	Amendment 3: Restart (SC21 has asked JTC1 for endorsement to cancel project)
ISO/IEC 9805-1	Information Technology - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Protocol, Edition 2, 1993 [SC21 N 8433] (X.852:1993)
DIS 9805-2.2♦	Information Technology - Open Systems Interconnection - Protocol Specification for the Commitment, Concurrency, and Recovery (CCR) Protocol, Part 2: CCR PICS Proforma, September 1993 (IS expected September 1994) (X.853:1993)
ISO 9807	Financial Transactions - Retail Banking Security - Requirements for Message Authentication, TC68/SC6/WG6
ISO/IEC 9834-1♦	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part 1: General Procedures, April 1993 (X.660:1992)
ISO/IEC 9834-1 PDAM 1	Amendment 1: Object Identifier Component Attribute Type in Annex B to Accommodate "Short Form Names"

ISO/IEC 9834-1 WDAM 2	Amendment 2: Incorporation of Definition of Root Arcs of Object Identifier Tree (PDAM December 1994, DAM December 1995, and AM December 1996)
ISO/IEC 9834-2•	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part 2: Registration Procedures for OSI Document Types, July 1993 [SC21 N 8149]
ISO/IEC 9834-3•	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part 3: Registration of Object Identifier Component Values for Joint ISO-CCITT Use, September 1990 [SC21 N 4718, April 1990] (X.662)
ISO/IEC 9834-3 WDAM 1	Amendment 1: Alignment with ISO/IEC 9834-1:1993 (PDAM December 1994, DAM December 1995, and AM December 1996)
ISO/IEC 9834-4•	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part 4: Register of VTE Profiles, November 1991
ISO/IEC 9834-5•	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part 5: Register of VT Control Objects Definitions, November 1991
ISO/IEC 9834-6•	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part 6: Registration of Procedures for Application Processes and Application Entities, November 1993 (X.665:1992)
WD 9834-7	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part D: Registration of Application Contexts, 1990 (work suspended by SC21, November 1989) (SC21 has asked JTC1 for endorsement to cancel the project)
WD 9834-8	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part E: Registration of System Titles, 1990 (will probably be incorporated in OSI management standards) (SC21 has asked JTC1 for endorsement to cancel the project)
WD 9834-11	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part F: Registration of Authentication Mechanisms, 1990 (WITHDRAWN; canceled by SC21, November 1989)
WD 9834-B	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part B: Registration of Abstract Syntaxes, 1990
WD 9834-C	Information Technology - Open Systems Interconnection - Procedures for the Operation of OSI Registration Authorities, Part C: Registration of Transfer Syntaxes, 1990
ISO 9899	Information Technology - Programming Languages - C, 1990 (ANSI/ISO 9899-1990)
ISO 9945-1	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1: System Application Program Interface (API), 1990
CD 9945-1.1	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1.1: Language Independent Base (WG15 work item based on IEEE P1003.1c)
CD 9945-1.2	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1.2: Real-time and Extensions (WG15 work item based on IEEE P1003.4 and .1b)
CD 9945-1.3	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1.3: Distribution Services (WG15 work item based on IEEE P1003.8)
CD 9945-1.3.1	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.1: Transparent File Access (WG15 work item based on IEEE P1003.8)
CD 9945-1.3.2	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.2: Remote Procedure Call (WG15 work item based on IEEE P1237)
CD 9945-1.3.3	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.3: Transport Interface (WG15 work item based on IEEE P1003.11)
CD 9945-1.3.4	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1.3.4: Name Space/Directory Services (WG15 work item based on IEEE P1003.12)
DIS 9945-2.1	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 2.1: Shell and Utilities (WG15 work item based on IEEE P1003.2)
CD 9945-2.2	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 2.2: User Portability Extensions (WG15 work item based on IEEE P1003.2a)
CD 9945-3	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 1: System Management
CD 9945-3.1	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 3.1: General Services (WG15 work item based on IEEE P1003.7)
CD 9945-3.2	Information Technology - Portable Operating System Interface for Computer Environments (POSIX), Part 3.2: Batch Services (WG15 work item based on IEEE P1003.10)
DP 9955	Methodology and Guidelines for the Development of Application Protocols for Banking Information Interchange [SC21 N 7706], 30 March 1993
ISO/IEC TR 9973	Information Processing - Procedures for Registration of Graphical Items, 1988
ISO 9979	Information Processing - Data Encipherment - Procedures for the Registration of Cryptographic Algorithms, 1991 [SC27 N 88]
DIS 9995-1	Information Technology, Keyboard Layouts for Text and Office Systems, Part 1: General Principles Governing Keyboard Layouts, 4 November 1991

DIS 9995-2	Information Technology, Keyboard Layouts for Text and Office Systems, Part 2: Alphanumeric Section, 4 November 1991
DIS 9995-3	Information Technology, Keyboard Layouts for Text and Office Systems, Part 3: Common Secondary Layout of Alphanumeric Zone of Alphanumeric Section, 4 November 1991
DIS 9995-4	Information Technology, Keyboard Layouts for Text and Office Systems, Part 4: Principles Governing the Placement of Characters and Symbols on Keys, 4 November 1991
DIS 9995-5	Information Technology, Keyboard Layouts for Text and Office Systems, Part 5: Editing Section, November 1991
DIS 9995-6	Information Technology, Keyboard Layouts for Text and Office Systems, Part 6: Functional Section, 4 November 1991
DIS 9995-7	Information Technology, Keyboard Layouts for Text and Office Systems, Part 7: Symbols Used to Represent Functions, 4 November 1991
DIS 9995-8	Information Technology, Keyboard Layouts for Text and Office Systems, Part 8: Allocation of Letters to the Keys of a Numeric Keyboard
ISO/IEC TR 10000-1◆	Information Technology - Framework and Taxonomy of International Standardized Profiles (ISPs), Part 1: Framework, Edition 2, 1992
WDTR 10000-1.3	Information Technology - Framework and Taxonomy of International Standardized Profiles (ISPs), Part 1: Taxonomy, Edition 3, July 1993
ISO/IEC TR 10000-2◆	Information Technology - Framework and Taxonomy of International Standardized Profiles, Part 2: Taxonomy of OSI Profile, Edition 2, November 1991 [SGFS N 430]
DTR 10000-2.3	Information Technology - Framework and Taxonomy of International Standardized Profiles, Part 2: Taxonomy of Profiles, Edition 3, August 1992
WDTR 10000-3	Information Technology - Framework and Taxonomy of International Standardized Profiles, Part 3: Principles and Taxonomy for OSE Profiles, August 1993
ISO/IEC 10021-1◆	Information Processing - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 1: System and Service Overview, 1990 (see X.400)
ISO/IEC 10021-1/Cor 1	Technical Corrigendum 1, 1991
ISO/IEC 10021-1/Cor 2	Technical Corrigendum 2, 1991
ISO/IEC 10021-1/Cor 3	Technical Corrigendum 3, 1992
ISO/IEC 10021-1/Cor 4	Technical Corrigendum 4, 1992
ISO/IEC 10021-1/Cor 5	Technical Corrigendum 5, 1992
ISO/IEC 10021-2◆	Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 2: Overall Architecture, 1990 (see X.402)
ISO/IEC 10021-2/Cor 1	Technical Corrigendum 1, 1991
ISO/IEC 10021-2/Cor 2	Technical Corrigendum 2, 1991
ISO/IEC 10021-2/Cor 3	Technical Corrigendum 3, 1992
ISO/IEC 10021-2/Cor 4	Technical Corrigendum 4, 1992
ISO/IEC 10021-2 PDAM 1	Amendment 1: Representation of O/R Addresses for Human Exchange, June 1991
ISO/IEC 10021-2 PDAM 2	Amendment 2: Minor Enhancements, June 1991
ISO/IEC 10021-3◆	Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 3: Abstract Service Definition Conventions, 1990 (see X.407)
ISO/IEC 10021-3/Cor 1	Technical Corrigendum 1, 1992
ISO/IEC 10021-4◆	Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 4: Message Transfer System: Abstract Service Definition and Procedures, 1990 (see X.411)
ISO/IEC 10021-4/Cor 1	Technical Corrigendum 1, 1991
ISO/IEC 10021-4/Cor 2	Technical Corrigendum 2, 1991
ISO/IEC 10021-4/Cor 3	Technical Corrigendum 3, 1992
ISO/IEC 10021-4/Cor 4	Technical Corrigendum 4, 1992
ISO/IEC 10021-4/Cor 5	Technical Corrigendum 5, 1992
ISO/IEC 10021-4 PDAM 1	Amendment 1: Minor Enhancements, June 1991
ISO/IEC 10021-5◆	Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 5: Message Store: Abstract Service Definition, 1990 (see X.413)
ISO/IEC 10021-5/Cor 1	Technical Corrigendum 1, 1991
ISO/IEC 10021-5/Cor 2	Technical Corrigendum 2, 1991
ISO/IEC 10021-5/Cor 3	Technical Corrigendum 3, 1992
ISO/IEC 10021-5/Cor 4	Technical Corrigendum 4, 1992
ISO/IEC 10021-5/Cor 5	Technical Corrigendum 5, 1992
ISO/IEC 10021-6◆	Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 6: Protocol Specifications, 1990 (see X.419)
ISO/IEC 10021-6/Cor 1	Technical Corrigendum 1, 1991
ISO/IEC 10021-6/Cor 2	Technical Corrigendum 2, 1991
ISO/IEC 10021-6/Cor 3	Technical Corrigendum 3, 1992
ISO/IEC 10021-6/Cor 4	Technical Corrigendum 4, 1992

ISO/IEC 10021-6/Cor 5 Technical Corrigendum 5, 1992

ISO/IEC 10021-7◆ Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 7: Interpersonal Messaging System, 1990 (see X.420)

ISO/IEC 10021-7/Cor 1 Technical Corrigendum 1, 1991

ISO/IEC 10021-7/Cor 2 Technical Corrigendum 2, 1991

ISO/IEC 10021-7/Cor 3 Technical Corrigendum 3, 1992

ISO/IEC 10021-7/Cor 4 Technical Corrigendum 4, 1992

ISO/IEC 10021-7/Cor 5 Technical Corrigendum 5, 1992

ISO/IEC 10021-7 PDAM 1 Amendment 1: Minor Enhancements, June 1991

ISO/IEC 10021-11 Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 11: MTS Routing, February 1991

ISO/IEC 10021-12 Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 12: PICS Proforma for Message Transfer Protocol, June 1991

ISO/IEC 10021-13 Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 13: PICS Proforma for Message Transfer Access Protocol, June 1991

ISO/IEC 10021-14 Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 14: PICS Proforma for Message Store Access Protocol, June 1991

ISO/IEC 10021-15 Information Technology - Text Communication - Message Oriented Text Interchange System (MOTIS), Part 15: PICS Proforma for Interpersonal Messaging, July 1991

ISO/IEC 10022◆ Information Technology - Open Systems Interconnection - Physical Service Definition (X.211), August 1990

ISO/IEC TR 10023◆ Information Technology - Telecommunications and Information Exchange Between Systems - Formal Description of ISO/IEC 8072 in LOTOS, 1992

ISO/IEC TR 10024◆ Information Technology - Telecommunications and Information Exchange Between Systems - Formal Description of ISO/IEC 8073 (Classes 0, 1, 2, 3) in LOTOS, 1992

ISO/IEC 10025-1◆ Information Technology - Telecommunications and Information Exchange Between Systems - Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network Service (CONS), Part 1: General Principles, 1993

ISO/IEC 10025-2◆ Information Technology - Telecommunications and Information Exchange Between Systems - Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network Service (CONS), Part 2: Test Suite Structure and Test Principles, 1993

ISO/IEC 10025-3◆ Information Technology - Telecommunications and Information Exchange Between Systems - Transport Conformance Testing for Connection Oriented Transport Protocol Operating over the Connection Oriented Network Service (CONS), Part 3: Transport Test Management Protocol Specification, 1993

ISO/IEC 10026-1◆ Information Technology - Open Systems Interconnection - Distributed Transaction Processing (TP), Part 1: Model, December 1992 [SC21 N 7457] (X.860:1992)

ISO/IEC 10026-1 PDAM 1 Amendment 1: Commitment Optimization, September 1993 [SC21 N 8219, 8220, 7649) (DAM expected June 1994; and AM expected June 1995)

ISO/IEC 10026-1/3 WDAMs Draft Amendments to Parts 1-3: Distributed Transaction Processing Dialogue Recovery and User Suspension of a Dialogue [SC21 N 6710] (PDAMs expected November 1995, DAMs November 1996, and AMs November 1997)

ISO/IEC 10026-1/3 WDAMs Draft Amendments to Parts 1-3: Transaction Processing Association Pool Management, WDAMs, February 1992 [SC21 N 7604] (formerly entitled Association Management) (PDAMs expected July 1994, DAM July 1995, and AM July 1996)

ISO/IEC 10026-1/3 WDAMs Draft Amendments to Parts 1-3: Transaction Processing Sub-Transactions, SC21/WG5, WDAMs, July 1991 [SC21 N 6236] (PDAMs expected November 1995, DAMs November 1996, and AMs November 1997)

ISO/IEC 10026-1/4 WDAMs Draft Amendments to Parts 1-3: Transaction Processing Separate Data and Commit Associations, WDAMs, July 1991 [SC21 N 6240] (PDAMs expected November 1995, DAMs November 1996, and AMs November 1997)

ISO/IEC 10026-1/3 WDAMs Draft Amendments to Parts 1-3: Transaction Processing Security, WDAMs, July 1991 [SC21 N 6232] (PDAMs expected November 1995; DAMs November 1996; and AMs November 1997)

ISO/IEC 10026-2◆ Information Technology - Open Systems Interconnection - Distributed Transaction Processing (TP), Part 2: Service, August 1992 [SC21 N 7304] (X.861:1992)

ISO/IEC 10026-2 PDAM 1 Amendment 1: Commitment Optimizations, September 1993 [SC21 N 8220]

ISO/IEC 10026-3◆ Information Technology - Open Systems Interconnection - Distributed Transaction Processing (TP), Part 3: Transaction Processing Protocol Specification, December 1992 [SC21 N 7518] (X.862)

ISO/IEC 10026-3 PDAM 1 Amendment 1: Commitment Optimizations, September 1993 [SC21 N 7649]

ISO/IEC 10026-4 Information Technology - Open Systems Interconnection - Distributed Transaction Processing (TP), Part 4: PICS Proforma, SC21/WG5, October 1993 [SC21 N 8290] (X.863)

ISO/IEC 10026-5 Information Technology - Open Systems Interconnection - Distributed Transaction Processing (TP), Part 5: Application Context Proforma, 1993

ISO/IEC 10026-6	Information Technology - Open Systems Interconnection - Distributed Transaction Processing (TP), Part 6: Unstructured Data Transfer, 1993
CD 10026-7	Information Technology - Open Systems Interconnection - Distributed Transaction Processing (TP), Part 7: Message Queueing, July 1993 [SC21 N 8148]
ISO/IEC 10027	Information Technology - Information Resource Dictionary System (IRDS) Framework, June 1990
WD 10027.2	Information Technology - Information Resource Dictionary System (IRDS) Framework, Edition 2 (revision to address new requirements and alignment with RMDM, SQL, RDA, Directory, and ODP), 1993 [SC21 N 8204] (CD expected July 1994)
ISO/IEC 10028-1◆	Definition of the Relaying Functions of a Network Layer Intermediate System, Part 1: Connection-mode Network Service, 1993
ISO/IEC 10028-1 PDAM 1	Amendment 1: Connectionless Mode Relaying Functions, February 1991
ISO/IEC 10028-2◆	Definition of the Relaying Functions of a Network Layer Intermediate System, Part 2: Connectionless Network Service, 1993
ISO/IEC TR 10029◆	Information Technology - Telecommunications and Information Exchange Between Systems - Operation of an X.25 Interworking Unit, March 1989
ISO/IEC 10030	Information Technology - Telecommunications and Information Exchange Between Systems - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO/IEC 8878 (X.25 PLP) [SC6 N 5006], October 1990
ISO/IEC 10030/Cor 1	Technical Corrigendum 1, 1992
ISO/IEC 10030 PDAM 1	Amendment 1: Dynamic Discovery of OSI NASP Addresses by End Systems (New Work Item)
ISO/IEC 10030 AM 2	PICS Proforma, 1992 (see DIS 10030-2)
ISO/IEC 10030 PDAM 3	Amendment 3: Specification of IS-SNARE Interactions, August 1991
DIS 10030-2	Information Technology - Telecommunications and Information Exchange Between Systems - End System to Intermediate System Routing Information Exchange Protocol for Use in Conjunction with ISO/IEC 8878 (X.25 PLP), Part 2: PICS Proforma, October 1991
ISO/IEC 10031-1	Information Processing - Text and Office Systems - Distributed-Office-Applications Model (DOAM), Part 1: General Model, 1991
ISO/IEC 10031-2	Information Processing - Text and Office Systems - Distributed-Office-Applications Model (DOAM), Part 2: Distinguished Object References and Associated Procedures, 1991
ISO/IEC 10032	Information Technology - Reference Model of Data Management, January 1992
DP 10033	Information Processing - Text and Office Systems - Recording of Documents Conforming to ISO/IEC 8613 on Flexible Disk Cartridges Conforming to ISO/IEC 9293, May 1988
ISO/IEC TR 10034	Guidelines for the Preparation of Conformity Clauses in Programming Language Standards, 1990
ISO/IEC 10035◆	Information Technology - Open Systems Interconnection - Connectionless ACSE Protocol Specification, July 1991 (X.237:1992)
ISO/IEC 10035 WDAM 1	Amendment 1: Extensions to Support the Extended Application Layer Structure, December 1993 [SC21/WG8 N 196]
DIS 10035-2	Information Technology - Open Systems Interconnection - Connectionless ACSE Protocol Specification, Part 2: PICS Proforma for Connectionless ACSE Protocol, November 1993 [SC21 N 7870 rev] (initiation of ITU-TS approval ballot expected November 1994) (X.257)
ISO/IEC 10036	Information Technology - Font Information Exchange - Procedure for Registration of Glyph and Glyph Collection Identifiers, 1993
ISO/IEC TR 10037	Information Technology - SGML and Text-Entry Systems - Guidelines for SGML Syntax-Directed Editing Systems, 1991
DIS 10038◆	Information Technology - Local Area Networks - MAC Sublayer Interconnection (MAC Bridging) (awaiting DIS ballot), December 1991
DIS 10038 PDAM 1	Amendment 1: Specification of Management Information for CMIP (awaiting PDAM ballot)
DIS 10038 DAM 2	Amendment 2: Source Routing Supplement, October 1991
ISO/IEC 10039◆	Information Technology - Open Systems Interconnection - Local Area Networks - MAC Service Definition, October 1990
ISO/IEC 10040◆	Information Technology - Open Systems Interconnection - Systems Management Overview, Edition 2, 1992 (X.701:1992)
ISO/IEC 10040/Cor 1	Technical Corrigendum 1, October 1993 [SC21 N 8291]
ISO/IEC 10040 AM 1	Amendment 1: Management Knowledge Management Architecture, January 1993 [SC21 N 7527] (passed DIS ballot October 1993; IS text awaits resolution of ballot comments)
ISO/IEC 10040 PDAM 2	Amendment 2: Management Domains Architecture, June 1993 [SC21 N 7946] (editing meeting April 1994)
ISO/IEC 10116	Information Technology - Modes of Operation for an N-bit Block Cipher Algorithm, 1991
DIS 10118-1	Information Technology - Security Techniques - Hash Functions, Part 1: General Model, SC27/WG2, 1993
DIS 10118-2	Information Technology - Security Techniques - Hash Functions, Part 2: Hashing Operation Using Symmetric Block-Cipher Algorithm, SC27/WG2, 1993
WD 10118-3	Information Technology - Security Techniques - Hash Functions, Part 3: Dedicated Hash Functions, SC27/WG2, SC27 N 223, 1993

WD 10118-4 Information Technology - Security Techniques - Hash Functions, Part 4: Hash Functions Using Modular Arithmetic, SC27/WG2 N 21, 1993

ISO/IEC 10126-1 Financial Transactions - Wholesale Banking Security - Procedures for Message Encipherment, Part 1: General Principles, TC68/SC2, 1993

ISO/IEC 10126-2 Financial Transactions - Wholesale Banking Security - Procedures for Message Encipherment, Part 2: DEA- Algorithms, TC68/SC2, 1993

WD 10148.3 Information Technology - Basic Remote Procedure Call (RPC) Using OSI Remote Operations (fast-track ballot failed and DIS 10148 was withdrawn (revised effort in DIS 11578, September 1993)

ISO 10149 Information Processing Systems - Data Interchange on Read-Only 120-mm Optical Data Disks (CD-ROM), August 1988

DIS 10161-2 Information and Documentation - Open Systems Interconnection - Interlibrary Loan Application Protocol Specification, Part 2: Protocol Implementation Conformance Statement Proforma, March 1993 [SC21 N 7657]

ISO/IEC 10162 Information and Documentation - Search and Retrieve Application Service Definition for Open Systems Interconnection, 1993

ISO/IEC 10163 Information and Documentation - Search and Retrieve Application Protocol Specification for Open Systems Interconnection, 1993

ISO/IEC 10164-1◆ Information Technology - Open Systems Interconnection - Systems Management, Part 1: Object Management Function, June 1993 (X.730:1992)

ISO/IEC 10164-1 DAM 1 Amendment 1: ICS Proforma (previously MOCS/PICS Proforma), September 1993 [SC21 N 8240] (editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994)

ISO/IEC 10164-2◆ Information Technology - Open Systems Interconnection - Systems Management, Part 2: State Management Function, June 1993 (X.731:1992)

ISO/IEC 10164-2 DAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8241] (editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994)

ISO/IEC 10164-3◆ Information Technology - Open Systems Interconnection - Systems Management, Part 3: Attributes for Representing Relationship, June 1993 (X.732:1992)

ISO/IEC 10164-3 DAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8242] (editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994)

ISO/IEC 10164-4◆ Information Technology - Open Systems Interconnection - Systems Management, Part 4: Alarm Reporting Function, December 1992 (X.733:1992)

ISO/IEC 10164-4 DAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8243] (editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994)

ISO/IEC 10164-5◆ Information Technology - Open Systems Interconnection - Systems Management, Part 5: Event Report Management Function, June 1993 (name changed from Management Service Control Function) (X.734:1992)

ISO/IEC 10164-5 DAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8244] (editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994)

ISO/IEC 10164-5 PDAM 2 Amendment 2: Enhanced Discriminator, August 1993 (editing meeting April 1994)

ISO/IEC 10164-6◆ Information Technology - Open Systems Interconnection - Systems Management, Part 6: Log Control Function, November 1993 (X.735:1992)

ISO/IEC 10164-6 DAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8245] (editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994)

ISO/IEC 10164-6 PDAM 2 Amendment 2: Enhanced Log, August 1993 (editing meeting April 1994)

ISO/IEC 10164-7◆ Information Technology - Open Systems Interconnection - Systems Management, Part 7: Security Alarm Reporting Function, May 1992 (X.736:1992)

ISO/IEC 10164-7 DAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8246] (editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994)

ISO/IEC 10164-8◆ Information Technology - Open Systems Interconnection - Systems Management, Part 8: Security Audit Trail Function, June 1993 (X.740:1992)

ISO/IEC 10164-8/Cor 1 Draft Technical Corrigendum 1, January 1994 [SC21 N 8427]

ISO/IEC 10164-9◆ Information Technology - Open Systems Interconnection - Systems Management, Part 9: Objects and Attributes for Access Control, November 1993 [SC21 N 7661] (editing meeting February 1994; initiation of ITU-TS approval ballot expected November 1994) (X.741)

DIS 10164-10.2 Information Technology - Open Systems Interconnection - Systems Management, Part 10: Usage Metering Function (formerly Accounting Meter Function), November 1993 [SC21 N 8238] (ballot closes February 1994; editing meeting July 1994; initiation of ITU-TS approval ballot expected November 1994) (X.742)

ISO/IEC 10164-10 WDAM 1 Amendment 1: ICS Proforma, 1993 (PDAM expected July 1994)

ISO/IEC 10164-11◆ Information Technology - Open Systems Interconnection - Systems Management, Part 11: Metric Objects and Attributes (formerly Workload Monitoring Function), March 1993 [SC21 N 7533] (X.739:1993)

ISO/IEC 10164-11 WDAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8162] (PDAM expected July 1994)

ISO/IEC 10164-11 WDAM 2 Amendment 2: Additional Metric Objects and Attributes, September 1993 [SC21 N 8161] (PDAM expected July 1994)

ISO/IEC 10164-12♦ Information Technology - Open Systems Interconnection - Systems Management, Part 12: Test Management Function, December 1992 [SC21 N 7452] (X.745:1993)

ISO/IEC 10164-12 PDAM 1 Amendment 1: ICS Proforma, November 1993 [SC21 N 8335]

ISO/IEC 10164-13♦ Information Technology - Open Systems Interconnection - Systems Management, Part 13: Summarization Function (formerly Measurement Summarization Function), September 1993 [SC21 N 8160] (X.738:1993)

ISO/IEC 10164-13 WDAM 1 Amendment 1: ICS Proforma, September 1993 [SC21 N 8163] (PDAM expected December 1993)

ISO/IEC 10164-13 WDAM 2 Amendment 2: Additional Summarization Scanners, July 1993 [SC21 N 7963] (PDAM expected December 1993)

DIS 10164-14.2 Information Technology - Open Systems Interconnection - Systems Management, Part 14: Confidence and Diagnostic Test Categories, January 1993 [SC21 N 7454] (editing meeting in October 1993 proposed a second DIS; initiation of ITU-TS approval ballot expected February 1994) (X.737)

DIS 10164-15 Information Technology - Open Systems Interconnection - Systems Management, Part 15: Scheduling Function, May 1993 [SC21 N 7683] (editing meeting February 1994; initiation of ITU-TS approval ballot expected November 1994) (X.746)

CD 10164-16.2 Information Technology - Open Systems Interconnection - Systems Management, Part 16: Management Knowledge Management, October 1993 [SC21 N 8310] (initiation of ITU-TS approval ballot expected November 1994) (X.750)

CD 10164-17 Information Technology - Open Systems Interconnection - Systems Management, Part 17: Change Over Function, January 1994 [SC21 N 8422] (initiation of ITU-TS approval ballot expected in 1997) (X.751)

CD 10164-19 Information Technology - Open Systems Interconnection - Systems Management, Part 19: Management Domain and Management Policy Management Function, January 1994 [SC21 N 8423] (initiation of ITU-TS approval ballot expected in 1997) (X.749)

WD 10164-ev.2 Information Technology - Open Systems Interconnection - Systems Management, Part ev: Enhanced Event Control Function, July 1992 [SC21 N 7958] (CD expected December 1993; initiation of ITU-TS approval ballot expected in 1997) (X.746)

WD 10164-mo Information Technology - Open Systems Interconnection - Systems Management, Part mo: Managed Objects for Supporting Upper Layers, January 1994 [SC21 N 8434]

WD 10164-rm.2 Information Technology - Open Systems Interconnection - Systems Management, Part mo: General Relationship Management Function, June 1993 [SC21 N 8040] (CD text expected December 1994, DIS June 1996, and IS June 1997) (X.747)

WD 10164-rtm Information Technology - Open Systems Interconnection - Systems Management, Part rtm: Response Time Monitoring Function, August 1990 [SC21 7970] (CD expected December 1995; initiation of ITU-TS approval ballot expected in 1998) (X.748)

WD 10164-sw Information Technology - Open Systems Interconnection - Systems Management, Part x: Software Management Function, September 1993 [SC21 N 8201] (CD expected December 1993; initiation of ITU-TS approval ballot expected in 1997) (X.744)

WD 10164-tm.2 Information Technology - Open Systems Interconnection - Systems Management, Part y: Time Management Function, July 1993 [SC21 N 7961] [JTC1 N 763] (new work item; standard will have two parts: representation of time and mechanisms for the distribution and synchronization of time; CD expected July 1994; initiation of ITU-TS approval ballot expected in 1998) (X.743)

ISO/IEC 10165-1♦ Information Technology - Open Systems Interconnection - Structure of Management Information, Part 1: Management Information Model, September 1993 (X.720:1992)

ISO/IEC 10165-1/Cor 1 Technical Corrigendum 1, December 1993 [SC21 N 8360]

ISO/IEC 10165-1 PDAM 1 Amendment 1: Generalization of Terms (formerly General Relationship Model), June 1993 [SC21 N 7947] (editing meeting February 1994)

ISO/IEC 10165-2♦ Information Technology - Open Systems Interconnection - Structure of Management Information, Part 2: Definition of Management Information, October 1992 (incorporated Part 3) (X.721:1992)

ISO/IEC 10165-2/Cor 1 Draft Technical Corrigendum 1, July 1993 [SC21 N 7953]

ISO/IEC 10165-2 PDAM 1.2 Amendment 1: Enhanced Discriminator and Log, January 1993 [SC21 N 7559] (WG4 recommended in October 1993 a second PDAM ballot; editing meeting April 1994)

ISO/IEC 10165-4♦ Information Technology - Open Systems Interconnection - Structure of Management Information, Part 4: Guidelines for the Definition of Managed Objects, September 1992 (X.722:1992)

ISO/IEC 10165-4 PDAM 1 Amendment 1: GDMO Extensions, July 1993 [SC21 N 7948] (editing meeting February 1994)

ISO/IEC 10165-4 PDAM 2 Amendment 2: Set By Create and Component Registration, 1993 (editing meeting February 1994)

ISO/IEC 10165-5♦ Information Technology - Open Systems Interconnection - Structure of Management Information, Part 5: Generic Management Information, March 1993 [SC21 N 7640] (previously entitled Generic Managed Objects) (X.723:1993)

ISO/IEC 10165-6♦ Information Technology - Open Systems Interconnection - Structure of Management Information, Part 6: Requirements and Guidelines for Management Information Conformance Statement (MICS) Proformas, June 1993 [SC21 N 7894] (X.724:1993)

ISO/IEC 10165-6 WDAM 1	Amendment 1: Manager Role Conformance, July 1993 [SC21 N 7964] (PDAM expected December 1994)
ISO/IEC 10165-6/Cor 1	Draft Technical Corrigendum 1, January 1994 [SC21 N 8428]
CD 10165-7.2◆	Information Technology - Open Systems Interconnection - Structure of Management Information, Part 7: General Relationship Model (formerly Management Information Register and Registration Procedures), September 1993 [SC21 N 8036] (in the absence of an editor and target dates, the old project, Management Information Register and Registration Procedures has been cancelled [Ref. SC21 N 7728 1993]; editing meeting February 1994; initiation of ITU-TS approval ballot expected June 1995) (X.725)
WD 10165-x	Information Technology - Open Systems Interconnection - Management Information in the Upper Layers, October 1993 [SC21 N 8178] (CD expected July 1994)
ISO/IEC 10166-1	Information Technology - Text and Office Systems - Document Filing and Retrieval (DFR), Part 1: Abstract Service Definition and Procedures, June 1991
ISO/IEC 10166-2	Information Technology - Text and Office Systems - Document Filing and Retrieval (DFR), Part 2: Protocol Specification, June 1991
ISO/IEC TR 10167◆	Information Technology - Open Systems Interconnection - Guidelines for the Application of Estelle, LOTOS and SDL, November 1991 (Z.110)
DIS 10168-1◆	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol, Part 1: Test Suite Structure and Test Purposes, January 1991 (IS expected December 1994)
CD 10168-2◆	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol, Part 2: Common Session Abstract Test Suite (formerly Generic Test Suite), September 1993 [SC21 N 8164] (ballot ends January 1994)
CD 10168-3◆	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol, Part 3: Abstract Test Suite for the CS Method (formerly Session Generic Test Suite), September 1993 [SC21 N 8164] (ballot ends January 1994)
DIS 10168-4◆	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol, Part 4: Session Test Management Protocol Specification, March 1991 [SC21 N 5026] (IS expected December 1994)
ISO/IEC 10169-1◆	Information Technology - Open Systems Interconnection - Conformance Test Suite for the ACSE Protocol, Part 1: Test Suite Structure and Test Purposes, November 1991
WD 10169-2	Information Technology - Open Systems Interconnection - Conformance Test Suite for the Session Protocol, Part 2: Common ACSE Abstract Test Suite (WD expected June 1994; CD October 1994; DIS October 1995; IS October 1996)
ISO/IEC 10170-1◆	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol, Part 1: Test Suite Structure and Test Purposes, April 1993 [SC21 N 7530]
WD 10170-2	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol, Part 2: FTAM Abstract Test Suite, June 1989 [SC21 N 3665] (CD text expected October 1994, DIS in October 1995, IS in October 1996)
WD 10170-3	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol, Part 3: ACSE Abstract Test Suite Embedded Under FTAM, 1989 (formal WD text expected June 1994, CD text in October 1994, DIS in October 1995, IS in October 1996)
WD 10170-4	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol, Part 4: Presentation Abstract Test Suite Embedded Under FTAM, 1989 (formal WD text expected June 1994, CD text in October 1994, DIS in October 1995, IS in October 1996)
WD 10170-5	Information Technology - Open Systems Interconnection - Conformance Test Suite for the FTAM Protocol, Part 5: Session Abstract Test Suite Embedded Under FTAM, 1989 (formal WD text expected June 1994, CD text in October 1994, DIS in October 1995, IS in October 1996)
ISO/IEC TR 10171	List of Standard Data Link Layer Protocols that Utilize HDLC Classes of Procedures (awaiting publication)
ISO/IEC TR 10171 PDAM 1	Amendment 1: Registration of XID Format Identifiers and Private Parameter Set Identifiers (ballot closed 10 March 1991)
ISO/IEC TR 10172◆	Information Technology - Telecommunications and Information Exchange Between Systems - Network/Transport Protocol Interworking Specification, February 1991
ISO/IEC 10173◆	Information Technology - Integrated Services Digital Network (ISDN) - Primary Access Connector at Reference Points S and T, March 1991
DTR 10174	Information Technology - Telecommunications and Information Exchange Between Systems - Logical Link Control (Type 2 Operation) Test Purposes, 1993
DIS 10175	Information Technology - Text and Office Systems - Document Printing Application (DPA), SC18/WG4
ISO/IEC TR 10176	Information Technology - Guidelines for the Preparation of Programming Language Standards, 1991
ISO/IEC 10177◆	Information Technology - Data Communications - Intermediate-System Support of the OSI Connection-Mode Network Service Using ISO/IEC 8208 in Accordance with ISO/IEC 10028, 1993
ISO/IEC TR 10178	Information Technology - Telecommunications and Information Exchange Between Systems - The Structure and Coding of Logical Control Link Addresses in Local Area Networks, 1992

ISO/IEC 10179	Document Style Semantics and Specification Language (DSSSL), 28 June 1991, awaiting publication
DIS 10180	Standard Page Description Language (SPFL), March 1991
CD 10181-1.2◆	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 1: Overview, August 1992 [SC21 N 7083] (DIS expected January 1994; IS September 1994; initiation of ITU-TS approval ballot expected November 1994) (X.810)
ISO/IEC 10181-2◆	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 2: Authentication Framework, December 1993 [SC21 N 7853] (passed DIS ballot in October 1993; initiation of ITU-TS approval ballot expected November 1994) (X.811)
ISO/IEC 10181-2 WDAM 1	Amendment 1: Authentication Elements, July 1991 [SC21 N 6172] (new work item in WG1)
DIS 10181-3◆	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 3: Access Control Framework, June 1992 [SC21 N 6947] (IS expected June 1994; initiation of ITU-TS approval ballot expected November 1994) (X.812)
DIS 10181-4◆	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 4: Non-Repudiation Framework, December 1993 [SC21 N 8378] (initiation of ITU-TS approval ballot expected November 1994) (X.813)
DIS 10181-5◆	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 5: Confidentiality Framework, February 1993 [SC21 N 7602] (initiation of ITU-TS approval ballot expected November 1994) (X.814)
DIS 10181-6◆	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 6: Integrity Framework, February 1993 [SC21 N 7603] (initiation of ITU-TS approval ballot expected November 1994) (X.815)
CD 10181-7.2◆	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 7: Security Audit Framework, March 1993 [SC21 N 7685] (initiation of ITU-TS approval ballot expected November 1994) (X.816)
WD 10181-8	Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems, Part 8: Key Management
DTR 10182	Binding Techniques for Programming Languages [SC22/WG11 N 754], February 1992
ISO/IEC TR 10183	Text and Office Systems - ODA and Interchange Format - Technical Report on ISO/IEC 8613 Implementation Testing, 1993
CD 10184-1.2	Terminal Management - Model, July 1991 [SC21 N 4176, June 1990] (project cancelled)
WD 10184-2	Terminal Management - Service, July 1991 [SC21 N 4176, June 1990] (project cancelled)
WD 10184-3	Terminal Management - Protocol, July 1991 [SC21 N 4176, June 1990] (project cancelled)
ISO/IEC 10202-1	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Card Life Cycle TC68/SC6/WG7, 1993
DIS 10202-2	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Transaction Process, TC68/SC6/WG7, 1993
CD 10202-3	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Cryptographic Key Relationship, TC68/SC6/WG7, 1993
ISO/IEC 10202-4	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Secure Application Modules, TC68/SC6/WG7, 1993
CD 10202-5	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Use of Algorithms, TC68/SC6/WG7, 1993
DIS 10202-6	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Cardholder Verification, TC68/SC6/WG7, 1993
WD 10202-7	Financial Transactions - Security Architecture - Security Architecture of Integrated Circuit Cards (ICCs), Part 1: Key Management, TC68/SC6/WG7, 1993
ISO/IEC 10206	Information Technology - Programming Languages - Extended Pascal, 1991
DIS 10222	Enhanced Small Device Interface, 1991
ISO/IEC 10279	Information Technology - Programming Languages - Full BASIC, 1991
CD 10303-11	Information Technology - Standard for the Exchange of Product Model Data (STEP), Part 11: EXPRESS
ISO/IEC 10538	Information Technology - Control Functions for Text Communication, 1991
ISO/IEC 10588	Information Technology - Use of the X.29 PLP in Conjunction with X.21/X.21 bis to Provide the OSI CONS, 1993
ISO/IEC 10589◆	Information Technology - Telecommunications and Information Exchange Between Systems - Intermediate System to Intermediate System Intra-domain Routing Information Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless Network Service (ISO 8473), 1992
ISO/IEC ISP 10607-1◆	Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by FTAM, December 1990
ISO/IEC ISP 10607-1 DAM 1	Amendment 1: Additional Specifications for COBOL Document Types, May 1993
ISO/IEC ISP 10607-2◆	Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part 2: Definition of Document Types, Constraint Sets and Syntaxes, December 1990 (reprinted April 1991 to correct error in Foreword)

ISO/IEC ISP 10607-2 DAM 1 Amendment 1: Additional Definitions, December 1991

ISO/IEC ISP 10607-2 DAM 2 Amendment 2: Additional Specifications for COBOL Document Types, May 1993

ISO/IEC ISP 10607-2 DAM 3 Amendment 3: FTAM Constraint Set and Document Type for CGM, February 1993

ISO/IEC ISP 10607-3• Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part 3: AFT 11 - Simple File Transfer Service (Unstructured), December 1990 (reprinted April 1991 to correct error in Foreword)

ISO/IEC ISP 10607-4• Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part 4: AFT 12 - Positional File Transfer Service, December 1991

ISO/IEC ISP 10607-4 DAM 1 Amendment 1: Additional Specifications for COBOL Document Types, May 1993

ISO/IEC ISP 10607-5• Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part 5: AFT 22 - Positional File Access Service, December 1991

ISO/IEC ISP 10607-5 DAM 1 Amendment 1: Additional Specifications for COBOL Document Types, May 1993

ISO/IEC ISP 10607-6• Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part 6: AFT 3 - File Management Service, December 1991

ISO/IEC ISP 10607-x Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part x: AFT 13 - Full File Transfer (Hierarchical), Draft, 1993

ISO/IEC ISP 10607-y Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part y: AFT 23 - Full File Access (Hierarchical), Draft, 1993

ISO/IEC ISP 10607-z Information Technology - International Standard Profiles AFT nn - File Transfer, Access and Management, Part z: AFT 4 - Filestore Management Profiles, Draft, 1993

ISO/IEC ISP 10608-1• Information Technology - International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 1: General Overview and Subnetwork-Independent Requirements, 1992

ISO/IEC ISP 10608-2• Information Technology - International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 2: TA51 Profile Including Subnetwork-Dependent Requirements for CSMA/CD Local Area Networks, 1992

DISP 10608-3 Information Technology - International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 3: TA 52, LAN, Token Bus: CLNS, 1993

ISO/IEC ISP 10608-4• Information Technology - International Standardized Profile TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 4: TA53, LLC1, Token Ring LAN, 1993

ISO/IEC ISP 10608-5• Information Technology - International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless-mode Network Service, Part 5: TA1111/TA1121 Profiles Including Subnetwork-Dependent Requirements for X.25 Packet Switched Data Networks Using Switched Virtual Circuits, 1992

DISP 10608-6• Information Technology - International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless Network Service, Part 6: TA54 Profile, FDDI LAN Subnetwork, 1993

DISP 10608-13 Information Technology - International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless Network Service, Part 13: LAN-Dependent Requirements for Token Ring MAC and PHY

DISP 10608-14• Information Technology - International Standardized Profiles TA nnnn - Connection-mode Transport Service over Connectionless Network Service, Part 14: MAC, PHY, PMD Sublayer Dependent State Management Requirements over FDDI LAN Subnetwork

ISO/IEC ISP 10609-1 Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 1: Subnetwork-type Independent Requirements for Group TB, 1992

ISO/IEC ISP 10609-2• Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 2: Subnetwork-type Independent Requirements for Group TC, 1992

ISO/IEC ISP 10609-3 Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 3: Subnetwork-type Independent Requirements for Group TD, 1992

ISO/IEC ISP 10609-4 Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 4: Subnetwork-type Independent Requirements for Group TE, 1992

ISO/IEC ISP 10609-5 Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 5: Definition of Profile TB 1111/TB 1121 (Peranent Access via PSTN/Digital Data Circuit or CSDN, respectively, Leased Line, Virutal Call, Transport Protocol Classes 0, 2, and 4), 1992

ISO/IEC ISP 10609-6• Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 6: Definition of Profile TC 1111/TC 1121 (Peranent Access via PSTN/Digital Data Circuit or CSDN, respectively, Leased Line, Virutal Call, Transport Protocol Classes 0 and 2), 1992

ISO/IEC ISP 10609-7	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 7: Definition of Profile TD 1111/TD 1121 (Peranent Access via PSTN/Digital Data Circuit or CSDN, respectively, Leased Line, Virutal Call, Transport Protocol Classs 0), 1992
ISO/IEC ISP 10609-8	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 8: Definition of Profile TE 1111/TE 1121 (Peranent Access via PSTN/Digital Data Circuit or CSDN, respectively, Leased Line, Virutal Call, Transport Protocol Classs 2), 1992
ISO/IEC ISP 10609-9♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 9: Subnetwork-type Dependent Requirements for Network Layer, Data Link Layer, and Physical Layer Concerning Permanent Access to a Packet Switched Data Network Using Virtual Call, 1992
pDISP 10609-10	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 10: LAN Subnetwork-Dependent Media-Independent Requirements, 1993
pDISP 10609-11	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 11: LAN Subnetwork-Dependent Media-Dependent Requirements, 1993
pDISP 10609-12	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 12: TC51 Profile, LLC2, CSMA/CD LAN - Trnasport Protocol Classes 0 and 2, 1993
pDISP 10609-13	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 13: TC53 Profile, LLC2, Token Ring LAN - Trnasport Protocol Classes 0 and 2,1993
pDISP 10609-14	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 14: COTS Classes 0 and 2, CONS, LLC2, Token Ring LAN, 1993
pDISP 10609-20	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 20: TC/TD nnnn, Overview of the Generalized Multipart ISP structure for TC and TD Group Profiles for OSI Usage of ISDN, February 1993 (review ended June 1993)
pDISP 10609-21	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 21: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer and Data Link Layer Concerning End Systems Attached to an ISDN Subnetwork for B-Channel X.25 DTE-to-DTE Operation, February 1993 (review ended June 1993)
pDISP 10609-22	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 22: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer and Data Link Layer Concerning End Systems Attached to an ISDN Subnetwork for B-Channel X.25 DTE-to-DCE Operation, February 1993 (review ended June 1993)
pDISP 10609-23	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 23: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer and Data Link Layer for Data Transfer Concerning Packet-Switched Mode ISDN Virtual Calls: B-Channel Access Case, February 1993 (review ended June 1993)
pDISP 10609-24	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 24: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer Using Q.931 - Circuit-Switched Case, February 1993 (review ended June 1993)
pDISP 10609-25	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 25: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Outgoing Call of a Packet-Switched Mode ISDN in Case B Using Virtual Calls, February 1993 (review ended June 1993)
pDISP 10609-26	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 26: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Outgoing Call of a Packet-Switched Mode ISDN in Case B Using Virtual Calls, February 1993 (review ended June 1993)
pDISP 10609-27	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 27: TC/TD nnnn, Subnetwork Type Dependent Requirements for Network Layer for Call Control Procedures Concerning the Incoming Call of a Packet-Switched Mode ISDN in Case B Using Virtual Calls, February 1993 (review ended June 1993)
pDISP 10609-28	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 28: TC/TD nnnn,

	Subnetwork Type Dependent Requirements for Data Link Layer for End Systems Attached to an ISDN Subnetwork, February 1993 (review ended June 1993)
pDISP 10609-29	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 29: TC 1131, ISDN B-Channel Virtual Call, Permanent Access to a PSDN - Transport Protocol Classes 0 and 2, February 1993 (review ended June 1993)
pDISP 10609-30	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 30: TC 1131, ISDN B-Channel Virtual Call, Switched Access to a PSDN - Transport Protocol Classes 0 and 2, February 1993 (review ended June 1993)
DISP 10609-31♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 31: TC 1231, ISDN B-Channel Virtual Call, Switched Access to a PSDN - Transport Protocol Classes 0 and 2, 1993
DISP 10609-32♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 32: TC 4111, ISDN B-Channel X.25 DTE to DTE, Semi-permanent Service - Transport Protocol Classes 0 and 2, 1993
DISP 10609-33♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 33: TC 4112, ISDN B-Channel X.25 DTE o DTE, Circuit-mode Service - Transport Protocol Classes 0 and 2, 1993
DISP 10609-34♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 34: TC 43111, ISDN D-Channel Access Virtual Call, Packet-mode Service, Without Q.931 - Transport Protocol Classes 0 and 2, 1993
DISP 10609-35♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 35: TC 43112, ISDN D-Channel Access Virtual Call, Packet-mode Service, with Q.931 - Transport Protocol Classes 0 and 2, 1993
DISP 10609-36♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 36: TC 43211, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, Without Q.931 - Transport Protocol Classes 0 and 2, 1993
DISP 10609-37♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 37: TC 43212, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, with Q.931 - Transport Protocol Classes 0 and 2, 1993
DISP 10609-38♦	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 38: TC 4331, ISDN B-Channel Demand Access Virtual Call, Packet-mode Service - Transport Protocol Classes 0 and 2, 1993
pDISP 10609-40	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 40: TD 1131, ISDN B-Channel Virtual Call, Permanent Access to a PSDN - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-41	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 41: TD 1231, ISDN B-Channel Virtual Call, Switched Access to a PSDN - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-42	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 42: TD 4111, ISDN B-Channel, X.25 DTE-to-DTE, Semi-Permanent Service - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-43	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 43: TD 4211, ISDN B-Channel, X.25 DTE-to-DTE, Circuit-mode Service - Transport Protocol Class 0, February 1993 (review ended June 1993)
pDISP 10609-44	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 44: TD 43111, ISDN D-Channel Access Virtual Call, Packet-mode Service, Without Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)
pDISP 10609-45	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 45: TD 43112, ISDN D-Channel Access Virtual Call, Packet-mode Service, With Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)
pDISP 10609-46	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 46: TD 43211, ISDN B-Channel Permanent Access Virtual Call, Packet-mode Service, Without Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)

pDISP 10609-47	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 47: TD 43212, ISDN B-Channel, Permanent Access Virtual Call, Packet-mode Service, With Q.931 - Transport Protocol Classes 0, February 1993 (review ended June 1993)
pDISP 10609-48	Information Technology - International Standardized Profiles TB, TC, TD, and TE - Connection-mode Transport Service over Connection-mode Network Service, Part 48: TD 43212, ISDN B-Channel, Demand Access Virtual Call, Packet-mode Service - Transport Protocol Classes 0, February 1993 (review ended June 1993)
ISO/IEC ISP 10610-1	Information Technology - International Standardized Profiles FOD nn, Part 1: FOD 11 Profile, Simple Document Structure - Character Content Only, April 1992
DISP 10611-1•	Information Technology - International Standardization Profiles AMH1n - Message Handling Systems - Common Messaging, Part 1: MHS Service Support, 1993
DISP 10611-2•	Information Technology - International Standardization Profiles AMH1n - Message Handling Systems - Common Messaging, Part 2: Specification of ROSE, RTSE, ACSE, Presentation, and Session Protocols for Use by MHS, 1993
DISP 10611-3•	Information Technology - International Standardization Profiles AMH1n - Message Handling Systems - Common Messaging, Part 3: AMH11: Message Transfer (P1), 1993
DISP 10611-4•	Information Technology - International Standardization Profiles AMH1n - Message Handling Systems - Common Messaging, Part 4: AMH12: MTS Access (P2), 1993
DISP 10611-5•	Information Technology - International Standardization Profiles AMH1n - Message Handling Systems - Common Messaging, Parat 5: AMH13: MS Access (P7), 1993
DISP 10612-1	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 1: RD 5p.5q Profile, Relaying MAC Using Transparent Bridging - General Overview and Subnetwork-Independent Requirements, 1993
DISP 10612-2	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 2: RD 5p.5q Profile, CSMA/CD LAN Subnetwork-Dependent Media-Dependent Requirements, 1993
pDISP 10612-3	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 3: RD 5p.5q Profile, Token Ring LAN Subnetwork-Dependent Media-Dependent Requirements, May 1993 (balloting ended September 1993)
DISP 10612-4•	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 4: RD 51.51 Profile, CSMA/CD LAN - CSMA/CD LAN, 1993
pDISP 10612-5	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 5: RD 51.54 Profile, CSMA/CD - FDDI, May 1993 (balloting ended September 1993)
pDISP 10612-6	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 6: RD 54.54 Profile, FDDI - FDDI, May 1993 (balloting ended September 1993)
pDISP 10612-7	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 7: RD 51.53 Profile, CSMA/CD LAN - Token Ring LAN, May 1993 (balloting ended September 1993)
pDISP 10612-8	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 8: RD 53.53 Profile, Token Ring LAN - Token Ring LAN, May 1993 (balloting ended September 1993)
pDISP 10612-9	Information Technology - International Standardized Profiles RD nn.nn - Relaying the MAC Service Using Transport Bridging, Part 9: RD 53.54 Profile, Token Ring LAN - FDDI LAN, May 1993 (balloting ended September 1993)
pDISP 10613-1•	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 1: Relay Function, Overview, Subnetwork-Indepenent Requirements, 1993
pDISP 10613-2•	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 2: LAN Subnetwork-Depdendent, Media-Independent Requirements, 1993
pDISP 10613-3•	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 3: CSMA/CD LAN Subnetwork-Dependent Media-Independent Requirements, 1993
DISP 10613-4	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 4: FDDI LAN Subnetwork-Dependent Media-Dependent Requirements, 1993 (review ended April 1993)
pDISP 10613-5•	Information Technology - International Standardized Profiles RA nn.nn -Relaying the Connectionless-mode Network Service, Part 5: RA51.51 Profile, CSMA/CD - CSMA/CD, 1993
pDISP 10613-6	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 6: RA 51.54, CSMA/CD LAN and FDDI LAN, 1993 (review ended April 1993)

pDISP 10613-7◆	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 7: PSDN Subnetwork-Dependent Media-Dependent Virtual Call Permanent Access, 1993
pDISP 10613-8◆	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 8: RA51.1111 Profile, CSMA/CD - PSTN, Permanent Access, PSTN-Leased Virtual Call, 1993
pDISP 10613-9◆	Information Technology - International Standardized Profiles RA nn.nn - Relaying the Connectionless-mode Network Service, Part 9: RA51.1121 Profile, CSMA/CD - PSTN, Permanent Access, CSDN-Leased Virtual Call, 1993
pDISP 10614-1	Information Technology - International Standardized Profiles RC nn.nn - Relaying X.25 PLP, Part 1: General Overview and Subnetwork-Independent Requirements, 1993
pDISP 10614-2	Information Technology - International Standardized Profiles RC nn.nn - Relaying X.25 PLP, Part 2: LAN Subnetwork-Dependent Media-Independent Requirements, 1993
pDISP 10614-3	Information Technology - International Standardized Profiles RC nn.nn - Relaying X.25 PLP, Part 3: CSMA/CD LAN Subnetwork-Dependent Media-Dependent Requirements, 1993
pDISP 10614-4	Information Technology - International Standardized Profiles RC nn.nn - Relaying X.25 PLP, Part 4: PSDN Subnetwork Type Dependent Requirements, 1993
DISP 10614-5◆	Information Technology - International Standardized Profiles RC nn.nn - Relaying X.25, Part 5, RC51.1111, CSMA/CD - PSDN Permanent Access PSTN-Leased Virtual Circuit, 1993
DISP 10614-6◆	Information Technology - International Standardized Profiles RC nn.nn - Relaying X.25, Part 6, RC51.1121, CSMA/CD - PSDN Permanent Access CSDN-Leased Virtual Circuit, 1993
DISP 10615-1◆	Information Technology - International Standardized Profiles ADI nn -- OSI Directory, Part 1: ADI 11, DUA Support of Directory Access, January 1993
DISP 10615-2◆	Information Technology - International Standardized Profiles ADI nn -- OSI Directory, Part 2: ADI 12, DSA Support of Directory Access, January 1993
DISP 10615-3◆	Information Technology - International Standardized Profiles ADI nn -- OSI Directory, Part 3: ADI 21, DSA Responder Role, July 1993
DISP 10615-4◆	Information Technology - International Standardized Profiles ADI nn -- OSI Directory, Part 4: ADI 22, DSA Initiator Role, July 1993
pDISP 10615-5	Information Technology - International Standardized Profiles ADI nn -- OSI Directory, Part 5: ADI 31, DUA Support of Distributed Operations, 1993
pDISP 10615-6	Information Technology - International Standardized Profiles ADI nn -- OSI Directory, Part 6: ADI 32, DSA Support of Distributed Operations, 1993
pDISP 10615-7	Information Technology - International Standardized Profiles ADI nn -- OSI Directory, Part 7: ADI 41, Strong Authentication, 1993
DISP 10616	Information Technology - International Standardized Profile FDI 11 - Directory Data Definitions - Common Directory Use (Normal), September 1993
ISO/IEC 10641	Information Technology - Open Systems Interconnection - Conformance Testing of Implementations of Graphics Standards, 1993
ISO/IEC 10646	Information Processing - Multiple Octet Coded Character Set, SC27, 14 November 1989 [SC21 N 4627], approved June 1992
ISO/IEC 10728	Information Resource Dictionary System (IRDS) Services Interface, April 1993
ISO/IEC 10728 PDAM 1	Amendment 1: C Language Binding, June 1993 [SC21 N 8088]
ISO/IEC 10728 WDAM 2	Amendment 2: Ada Language Binding, September 1993 [SC21 N 8203] (PDAM expected July 1994)
WD 10728.2	Information Resource Dictionary System (IRDS) Services Interface, Edition 2, 1993 (NWI Proposal October 1990; CD expected July 1994)
ISO/IEC 10729-1	Conformance Test Suite for the Presentation Protocol, Part 1: Test Suite Structure and Test Purposes for the Presentation Protocol, SC21/WG6, September 1993 [SC21 N 7872]
DIS 10729-2	Conformance Test Suite for the Presentation Layer, Part 2: Test Suite for ASN.1 Encodings and Test Purposes for Presentation Protocol, November 1993 [SC21 N 8232] (IS expected September 1994)
WD 10729-3	Conformance Test Suite for the Presentation Layer, Part 3: Common Presentation Abstract Test Suite, October 1991 (WD expected in June 1994; CD October 1994; DIS October 1995; IS October 1996)
ISO/IEC TR 10730	Information Technology - Open Systems Interconnection - Tutorial on Naming and Addressing, April 1993 [SC21 N 7460]
ISO/IEC TR 10730 WDAM 1	Amendment 1: Directory Names, June 1993 [SC21 N 7998] (dependent on progression of amendment to ISO/IEC 9834-1)
ISO/IEC 10731◆	Information Technology - Open Systems Interconnection - Conventions for the Definition of OSI Services, 1992 (ITU-TS ballot closed November 1993) (X.210:1993)
ISO/IEC 10732	Use of X.25 PLP to Provide the OSI CONS over the Telephone Network, 1993
ISO/IEC 10733◆	Information Technology - Telecommunications and Information Exchange Between Systems - Elements of Management Information Related to OSI Network Layer Standards, 1993
PDTR 10734	Guidelines for Bridged LAN Source Routing Operation by End Systems, 1991
ISO/IEC TR 10735	Standard Group MAC Addresses, 1993

ISO/IEC 10736	Information Technology - Open Systems Interconnection - Transport Layer Security Protocol, October 1993
DIS 10736 PDAM 1	Amendment 1, Security Association Establishment Protocol, JTC1/SC6, July 1991
ISO/IEC 10737◆	Information Technology - Telecommunications and Information Exchange Between Systems - Specification of the Elements of Management Information Related to OSI Transport Layer Standards, 1993
ISO/IEC TR 10738	Information Technology - Local and Metropolitan Area Networks - Token Ring Access Method and Physical Layer Specifications - Recommended Practice for Use of Unshielded Twisted Pair Cable (UTP) for Token Ring Data Transmission at 4 Mbit/s, 1993 [ANSI/IEEE 802.5b-1991]
ISO/IEC 10739-1	Information Technology - Open Systems Interconnection - Conformance Test Suite for 9041 - Virtual Terminal Basic Class Protocol, Part 1: Test Suite Structure and Test Purposes, 1992
ISO/IEC 10740-1	Information Technology - Text and Office Systems - Referenced Data Transfer, Part 1: Abstract Service Definition, 1993
ISO/IEC 10740-2	Information Technology - Text and Office Systems - Referenced Data Transfer, Part 2: Protocol Specification, 1993
DIS 10742	Information Technology - Telecommunications and Information Exchange Between Systems - Specification of the Elements of Management Information Related to OSI Data Link Layer Standards, 1993
CD 10743	Information Technology - Standard Music Description Language (SMDL), April 1991
ISO/IEC 10744	Information Technology - Hypermedia/Time-based Structuring Language (HyTime), 1992
ISO/IEC 10745◆	Information Technology - Open Systems Interconnection - Upper Layer Security Model, November 1993 [SC21 N 8334] (X.803)
WD 10746-1	Basic Reference Model for Open Distributed Processing, Part 1: Overview and Guide to Use (formerly Overview, now merged with old Part 4), September 1993 [SC21 N 7053] (CD expected July 1994, DIS in January 1995, and IS in October 1996) (X.901)
CD 10746-2.3	Basic Reference Model for Open Distributed Processing, Part 2: Descriptive Model, August 1993 [SC21 N 7988] (DIS expected February 1994 and IS November 1995) (X.902)
CD 10746-3.2	Basic Reference Model for Open Distributed Processing, Part 3: Prescriptive Model, August 1993 [SC21 N 8125] (DIS is expected in February 1994 and IS in November 1995) (X.903)
WD 10746-4	Basic Reference Model for Open Distributed Processing, Part 4: Architectural Semantics, Specification Techniques and Formalisms, August 1992 [SC21 N 7056] (CD text expected July 1994, DIS in January 1995, and IS in October 1996) (X.904)
DIS 10747◆	Information Technology - Telecommunications and Information Exchange Between Systems - Protocol for Exchange of Inter-Domain Routing Information Among Intermediate Systems to Support Forwarding of ISO/IEC 8473 PDUs, 1993
WD 10778	High-Speed Integrated Services Networks and User/Network Interface to High-Speed Integrated Services Networks
ISO/IEC 10918-1	Digital Compression and Coding of Continuous-Tone Still Images, Part 1: Requirements and Guidelines, 1993
DIS 10918-2	Digital Compression and Coding of Continuous-Tone Still Images, Part 2: Compliance Testing, 1993 (IS status expected March 1994)
WD 10918-3	Digital Compression and Coding of Continuous-Tone Still Images, Part 2: Extensions, 1993 (CD status expected December 1994, DIS in April 1995, and IS in 1996)
CD 10967-1	Information Technology - Programming Languages, Their Environments and Systems Software Interfaces - Language Compatible Arithmetic, Part 1: Integer and Floating Point Arithmetic, undergoing second review (November 1992-January 1993)
WD 10967-2	Information Technology - Programming Languages, Their Environments and Systems Software Interfaces - Language Compatible Arithmetic, Part 2: Complex Arithmetic and Mathematical Procedures
DIS 10994	Information Technology - Data Interchange on 90 mm Flexible Disk Cartridges Using MFM Recording at 31 831 FTPRAD on 80 Tracks on Each Side, June 1991
ISO/TR 11065	Industrial Automation Glossary, 1992
ISO/IEC 11072	Information Technology - Computer Graphics - Reference Model of Computer Graphics, 1992
ISO 11103	Space Data and Information Transfer Systems - Radio Metric and Orbit Data, 1991
ISO 11104	Space Data and Information Transfer Systems - Time Code Formats, 1991
ISO/IEC 11131	Financial Transactions - Wholesale Banking Security - Sign-On Authentication, TC68/SC2, 1993
DIS 11166-1	Financial Transactions - Wholesale Banking Security - Key Management by Means of Asymmetric Algorithms, Part 1: Principles, Procedures, and Formats, TC68/SC2, 1993
DIS 11166-2	Financial Transactions - Wholesale Banking Security - Key Management by Means of Asymmetric Algorithms, Part 2: Approved Algorithms Using RSA Cryptosystem, TC68/SC2, 1993
ISO/IEC 11172-1	Information Technology - Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 1: Systems, August 1993
ISO/IEC 11172-2	Information Technology - Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 2: Video, August 1993
ISO/IEC 11172-3	Information Technology - Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 3: Audio, August 1993

CD 11172-4	Information Technology - Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 4: Conformance Testing, November 1993 (DIS expected March 1994, IS in November 1994)
WD 11172-5	Information Technology - Coding of Moving Pictures and Associated Audio for Digital Storage Media at Up to about 1.5 Mbit/s, Part 5: Technical Report on Software for ISO/IEC 11172, 1993 (CD expected March 1994, DIS in July 1994, and IS in March 1995)
WD 11179-1.3	Information Technology - Coordination of Data Elements, Part 1: Framework for the Generation and Standardization of Data Elements, November 1993 (new WD expected March 1994)
WD 11179-2.2	Information Technology - Coordination of Data Elements, Part 2: Classification of Concepts for the Identification of Domains, November 1993 (new WD expected March 1994)
DIS 11179-3	Information Technology - Coordination of Data Elements, Part 3: Data Element Attributes, November 1993 (balloting ended February 1994)
DIS 11179-4	Information Technology - Coordination of Data Elements, Part 4: Definition of Data Elements, Janaury 1994
CD 11179-5.2	Information Technology - Coordination of Data Elements, Part 5: Naming Principles for Data Elements, Janaury 1994
CD 11179-6	Information Technology - Coordination of Data Elements, Part 6: Representation of Data Elements (Types), November 1993 (new WD expected March 1994)
ISO/IEC ISP 11181-1	Information Technology - International Standardized Profile FOD26 - Enhanced Document Structure - Character, Raster Graphics and Geometric Graphics Content Architecture, April 1992
ISO/IEC ISP 11182-1	Information Technology - International Standardized Profile FOD36 - Extended Document Structure - Character, Raster Graphics and Geometric Graphics Content Architecture, April 1992
ISO/IEC ISP 11183-1•	Information Technology - International Standardized Profiles AOM 1n - OSI Management - Management Communications Protocols, Part 1: Specification of ACSE, Presentation and Session Protocols for the Use by ROSE and CMISE, Revised Edition, December 1992
ISO/IEC ISP 11183-2•	Information Technology - International Standardized Profiles AOM 1n - OSI Management - Management Communications Protocols, Part 2: CMISE/ROSE for AOM 12, Enhanced Management Communications, 1993
pDISP 11183-x	Information Technology - International Standardized Profiles AOM 1n - OSI Management - Management Communications Protocols, Part x: Development of PTS for CMIP (AOM 11, AOM 12), 1993
pDISP 11184-1	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 1: FVT 121. S-mode Forms VTE Profile, 1993
pDISP 11184-2	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 2: FVT 122. S-mode Paged VTE Profile, 1993
pDISP 11184-3	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 3: FVT 111. A-mode Telnet Profile (pDISP expected 1995)
pDISP 11184-4	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 4: FVT 112. A-mode Scroll VTE Profile (pDISP expected 1995)
pDISP 11184-5	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 5: FVT 113. A-mode CCITT X.3 PAD Interworking (pDISP expected 1995)
pDISP 11184-6	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 6: FVT 114. A-mode Transparent VTE Profile (pDISP expected 1995)
pDISP 11184-7	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part 7: FVT 115. A-mode Generalized Telnet VTE Profile, 1993
pDISP 11184-x	Information Technology - International Standardized Profiles FVT 1nn - Virtual Terminal Basic Class - Register of VTE Profiles, Part x: FVT FVT 121 and 122: S-mode Forms and Paged VTE Profiles, 1993
DISP 11185-1	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 1: FVT 211, FVT 212, Sequenced and Unsequenced Application Control Objects, August 1993
DISP 11185-2	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 2: FVT 213, FVT 214, Sequenced and Unsequenced Terminal Control Objects, August 1993
DISP 11185-3	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 3: FVT 215, FVT 216, Application RIO Record Locating Control Object and Terminal RIO Record Notification Control Object, August 1993
DISP 11185-4	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 4: FVT 217, Horizontal Tabulation Control Object, August 1993
DISP 11185-5	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 5: FVT 218, Logical Image Control Object, August 1993

DISP 11185-6	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 6: FVT 219, Status Message Control Object, August 1993
DISP 11185-7	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 7: FVT 220, Entry-Control Control Object, August 1993
DISP 11185-8	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 8: FVT 221, Forms Field Entry Instruction Control Object (FEICO) No. 1, August 1993
DISP 11185-9	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 9: FVT 222, Paged Field Entry Instruction Control Object (FEICO) No. 1, August 1993
DISP 11185-10	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 10: FVT 231, Forms Field Entry Pilot Control Object (FEPCO) No. 1, 1993
DISP 11185-11	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 11: FVT 232, Paged Field Entry Pilot Control Object (FEPCO) No. 1, 1993
pDISP 11185-12	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 12: FVT FVT 2116, 2117, 2118, and 2119: Generalized Telnet Synchronization, Signal, Negotiation and Subnegotiation Control Objects (pDISP expected 1995)
pDISP 11185-13	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 13: FVT 2111, Waiting Time Control Object (pDISP expected 1995)
pDISP 11185-14	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 14: FVT 2112, Printer Control Object, 1993
pDISP 11185-15	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 15: FVT 2113, Field definition Control Object, 1993
pDISP 11185-16	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 16: FVT 2114, Terminal Signal Titles Control Object, 1993
pDISP 11185-17	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part 17: FVT 2115, Form Help Text Control Object, 1993
pDISP 11185-x	Information Technology - International Standardized Profiles FVT 2nn - Virtual Terminal Basic Class - Register of VT Control Objects, Part x: FVT 251, Terminal Conditions Control Object, 1993
pDISP 11186-1	Information Technology - International Standardized Profiles FVT 3nn - Virtual Terminal Basic Class - Register of Assignment Type Definitions, Part 1: FVT 321, Font Assignment Type No. 1 (DISP expected 1995)
DISP 11187-1◆	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 1: AVT 22, S-mode Forms Application Profile, 1993
DISP 11187-2◆	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 2: AVT 23, S-mode Paged Application Profile, 1993
pDISP 11187-3	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 3: S-mode ISPICS Requirements List No. 1 (pDISP expected 1995)
pDISP 11187-4	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 4, S-mode ISPICS Requirements (IPRL) List No. 1, Supporting Layers List No. 1 (pDISP expected 1995)
pDISP 11187-6	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 6: AVT 13, A-mode Scroll Application Profile, pDISP expected 1995-
pDISP 11187-7	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 7: AVT 14, A-mode CCITT X.3 PAD Application Profile (pDISP expected 1995)
pDISP 11187-8	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 8: AVT 15, A-mode Transparent Application Profile (pDISP expected 1995)
pDISP 11187-9	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 9: AVT 16, A-mode Generalized Telnet Application Profile, 1993
pDISP 11187-10	Information Technology - International Standardized Profiles AVT 1n, AVT 2n - Virtual Terminal Basic Class - Application Profiles, Part 10: AVT 17, A-mode ISPICS Requirements List No. 1 (pDISP expected 1995)

pDISP 11188-1	Information Technology - International Standardized Profiles - Common Upper Layer Requirements, Part 1: Basic Connection Oriented Requirements, July 1993
pDISP 11188-2	Information Technology - International Standardized Profiles - Common Upper Layer Requirements, Part 2: ROSE Based Requirements, October 1993 (pDISP status expected 1995)
pDISP 11188-3	Information Technology - International Standardized Profiles - Common Upper Layer Requirements, Part 3: Minimal OSI Upper Layer Facilities, July 1993
DISP 11189	Information Technology - International Standardized Profile FDI2 - Directory Data Definitions - MHS Use of Directory, September 1993
DISP 11190	Information Technology - International Standardized Profile FDI3 - Directory Data Definitions - FTAM Use of Directory, September 1993
ISO/IEC 11319	Information Technology - 8 mm Wide Magnetic Tape Cartridge for Information Interchange -- Helical Scan Recording, 1993
DIS 11321	Information Technology - 3,81 mm Wide Magnetic Tape Cartridge for Information Interchange -- Helical Scan Recording-- Data/Data Format, June 1991
ISO/IEC 11404	Information Technology - Programming Languages - Common Language-Independent Data Types (CLID), 1991
ISO/IEC 11544	Coded Representation of Bi-level and Limited Bits-per-pixel Still Pictures, 1993
ISO/IEC 11558	Information Technology - Data Compression for Information Interchange - Adaptive Coding with Embedded Dictionary, DCLZ Algorithm, 1992
DIS 11568-1	Financial Transactions - Retail Banking Security - Key Management, Part 1: Introduction to Key Management, TC68/SC6/WG6, 1993
DIS 11568-1	Financial Transactions - Retail Banking Security - Key Management, Part 1: Introduction to Key Management, TC68/SC6/WG6, 1993
DIS 11568-2	Financial Transactions - Retail Banking Security - Key Management, Part 2: Key Management Techniques for Symmetric Ciphers, TC68/SC6/WG6, 1993
DIS 11568-3	Financial Transactions - Retail Banking Security - Key Management, Part 3: Key Life Cycle for Symmetric Ciphers, TC68/SC6/WG6, 1993
WD 11568-5	Financial Transactions - Retail Banking Security - Key Management, Part 5: Key Management Techniques for Asymmetric Ciphers, TC68/SC6/WG6, 1993
WD 11568-6	Financial Transactions - Retail Banking Security - Key Management, Part 6: Key Life Cycle for Asymmetric Ciphers, TC68/SC6/WG6, 1993
WD 11568-7	Financial Transactions - Retail Banking Security - Key Management, Part 7: Key Management Schemes, TC68/SC6/WG6, 1993
CD 11568-8	Financial Transactions - Retail Banking Security - Key Management, Part 8: Key Management Related Data Elements, TC68/SC6/WG6, 1993
ISO/IEC 11569	Information Technology - Telecommunications and Information Exchange Between Systems - 26-Pole Interface Connector Mateability Dimensions and Contact Number Assignments, 1993
ISO/IEC 11570♦	Information Technology - Telecommunications and Information Exchange Between Systems - Transport Protocol Identification Mechanism, 1992
CD 11571	Information Technology - Telecommunications and Information Exchange Between Systems - Addressing in Private Integrated Services Digital Network, September 1991
CD 11572	Information Technology - Telecommunications and Information Exchange Between Systems - Addressing in Private Integrated Services Network - Circuit Mode Bearer Services - Inter-Exchange Signalling Procedures and Protocol, September 1991
CD 11573	Information Technology - Telecommunications and Information Exchange Between Systems - Synchronization Methods and Technical Requirements for Private Integrated Services Networks, September 1991
CD 11574	Information Technology - Telecommunications and Information Exchange Between Systems - Private Integrated Services Network - Circuit Mode 64 kbit/s Bearer Services - Service Definition - Functional Capabilities and Information Flows, September 1991
DIS 11577♦	Network Layer Security Protocol, JTC1/SC6, 1993
DIS 11578-1♦	Information Technology - Open Systems Interconnection - Remote Procedure Call, Part 1: Model, October 1993 [SC21 N 8212] (IS expected September 1994)
DIS 11578-2♦	Information Technology - Open Systems Interconnection - Remote Procedure Call, Part 2: Interface Definition Notation, October 1993 [SC21 N 8213] (IS expected September 1994)
DIS 11578-3♦	Information Technology - Open Systems Interconnection - Remote Procedure Call, Part 3: Service Definition, October 1993 [SC21 N 8214] (IS expected September 1994)
DIS 11578-4♦	Information Technology - Open Systems Interconnection - Remote Procedure Call, Part 4: Protocol Specification, October 1993 [SC21 N 8215] (IS expected September 1994)
WD 11578-5	Information Technology - Open Systems Interconnection - Remote Procedure Call, Part 5: PICS Proforma, June 1991 [SC21 N 6111] (formal WD expected July 1993; CD December 1993; DIS July 1994; IS July 1995; SC21 is considering canceling project in the absence of an editor and WD)
DIS 11586-1	Information Technology - Open Systems Interconnection - Generic Upper Layers Security (GULS), Part 1: Overview, Models and Notation, October 1993 [SC21 N 8182] (initiation of ITU-TS approval ballot expected November 1994) (X.830)

DIS 11586-2	Information Technology - Open Systems Interconnection - Generic Upper Layers Security (GULS), Part 2: Security Exchange Service Element (SESE) Service Definition, October 1993 [SC21 N 8183] (initiation of ITU-TS approval ballot expected November 1994) (X.831)
DIS 11586-3	Information Technology - Open Systems Interconnection - Generic Upper Layers Security (GULS), Part 3: Security Exchange Service Element (SESE) Protocol Specification, October 1993 [SC21 N 8184] (initiation of ITU-TS approval ballot expected November 1994) (X.832)
DIS 11586-4	Information Technology - Open Systems Interconnection - Generic Upper Layers Security (GULS), Part 4: Protecting Transfer Syntax Specification, October 1993 [SC21 N 8185] (initiation of ITU-TS approval ballot expected November 1994) (X.833)
WD 11586-5	Information Technology - Open Systems Interconnection - Generic Upper Layers Security (GULS), Part 5: SESE PICS Proforma, June 1993 [SC21 N 7912] (CD expected July 1994; initiation of ITU-TS approval ballot expected November 1994) (X.834)
WD 11586-6	Information Technology - Open Systems Interconnection - Generic Upper Layers Security, Part 6: Protecting Transfer Syntax - PICS Proforma, June 1993 [SC21 N 7913] (CD expected July 1994; initiation of ITU-TS approval ballot expected November 1994) (X.835)
CD 11587.2	Application Context for Systems Management with Transaction Processing, July 1993 [SC21 N 7899] (editing meeting February 1994; initiation of ITU-TS approval ballot expected June 1995) (X.702)
PDTR 11589	LOTOS Description of the CCR Service, June 1993 [SC21 N 7876]
PDTR 11590	LOTOS Description of the CCR Protocol, June 1993 [SC21 N 7877]
CD 11714	General Principles for the Creation of Symbols for Use in Technical Documentation of Products, September 1991
DIS 11730	Form Interface Management System (FIMS), 15 July 1992
ISO/IEC 11756	Information Technology, Programming Languages - MUMPS, 1992
WD 11770-1	Information Technology - Security Techniques - Key Management, Part 1: Framework, SC27/WG1, 1993 [SC27 N 685]
CD 11770-2	Information Technology - Security Techniques - Key Management, Part 2: Key Management Mechanisms Using Symmetric Techniques, SC27/WG2, November 1992 [SC27 N 626]
CD 11770-3	Information Technology - Security Techniques - Key Management, Part 3: Key Management Mechanisms Using Asymmetric Techniques, SC27/WG2, 1993
DISP 12059-0	Information Technology - International Standardized Profiles - Management Functions - Common Information for Management Functions, Part 0: Common Definitions for Management Function Profiles, December 1992 (ISP expected December 1993)
DISP 12059-1♦	Information Technology - International Standardized Profiles - Management Functions - Common Information for Management Functions, Part 1: Object Management, December 1992 (ISP expected December 1993)
DISP 12059-2♦	Information Technology - International Standardized Profiles - Management Functions - Common Information for Management Functions, Part 2: State Management, December 1992 (ISP expected December 1993)
DISP 12059-3♦	Information Technology - International Standardized Profiles - Management Functions - Common Information for Management Functions, Part 3: Attributes for Representing Relationships, December 1992 (ISP expected December 1993)
DISP 12059-4♦	Information Technology - International Standardized Profiles - Management Functions - Common Information for Management Functions, Part 4: Alarm Reporting, December 1992 (ISP expected December 1993)
DISP 12059-5♦	Information Technology - International Standardized Profiles - Management Functions - Common Information for Management Functions, Part 5: Event Report Management, December 1992 (ISP expected December 1993)
DISP 12059-6♦	Information Technology - International Standardized Profiles - Management Functions - Common Information for Management Functions, Part 6: Log Control, December 1992 (ISP expected December 1993)
DISP 12060-1♦	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part 1: AOM 211, General Management Capability, December 1992 (ISP expected December 1993)
DISP 12060-2	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part 2: AOM 212, Alarm Reporting and State Management Capabilities, December 1992 (ISP expected December 1993)
DISP 12060-3	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part 3: AOM 213, Alarm Reporting Capabilities, December 1992 (ISP expected December 1993)
DISP 12060-4♦	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part 4: AOM 221, General Event Report Management, December 1992 (ISP expected December 1993)
DISP 12060-5♦	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part 5: AOM 231, General Log Control, December 1992 (ISP expected December 1993)

pDISP 12060-w	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part w: AOM 242, Security Protocols (ISP expected November 1993)
pDISP 12060-x	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part x: AOM 251, General Performance Profile (ISP expected September 1994)
pDISP 12060-y	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part y: AOM 252x, Metric Objects (ISP expected May 1994)
pDISP 12060-z	Information Technology - International Standardized Profiles AOMnnn - OSI Management - Management Functions, Part z: AOM 253x, Summarization Objects (ISP expected September 1994)
DISP 12061-1	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 1: Introduction to the Transaction Processing Profiles, July 1993
DISP 12061-2	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 2: Support of the OSI TP APDUs, July 1993
DISP 12061-3	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 3: Support of the CCR Protocol, July 1993
DISP 12061-4	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 4: Support of Session, Presentation and ACSE Protocols, July 1993
DISP 12061-5	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 5: ATP 11, Application-Supported Transactions with Polarized Control, July 1993
DISP 12061-6	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 6: ATP 12, Application-Supported Transactions with Shared Control, July 1993
DISP 12061-7	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 7: ATP 21, Provider-Supported Transactions in Unchained Mode with Polarized Control, July 1993
DISP 12061-8	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 8: ATP 22, Provider-Supported Transactions in Unchained Mode with Shared Control, July 1993
pDISP 12061-9	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 9: ATP 31, Provider-Supported Transactions in Chained Mode with Polarized Control, July 1993 (ballot ended November 1993)
pDISP 12061-10	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 10: ATP 32, Provider-Supported Transactions in Chained Mode with Shared Control, July 1993 (ballot ended November 1993)
pDISP 12061-11	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part 11: TP Transaction Recovery Application Context, September 1993
pDISP 12061-x	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part x: Systems Profiling for TP, 1993
pDISP 12061-y	Information Technology - International Standardized Profiles ATP nn - OSI Distributed Transaction Processing, Part y: Development of PTS for TP, 1993
pDISP 12062-1	Information Technology - International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 1: IPM MHS Service Support, August 1993 (review ended December 1993)
pDISP 12062-2	Information Technology - International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 2: AMH 21, IPM Content, August 1993 (review ended December 1993)
pDISP 12062-3	Information Technology - International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 3: AMH 22, IPM Requirements for Message Transfer (P1), August 1993 (review ended December 1993)
pDISP 12062-4	Information Technology - International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 4: AMH 23, IPM Requirements for MTS Access (P3), August 1993 (review ended December 1993)
pDISP 12062-5	Information Technology - International Standardized Profiles AMH nn - Message Handling Systems - Interpersonal Messaging, Part 5: IPM Requirements for Enhanced MS Access (P7), August 1993 (review ended December 1993)
pDISP 12063	Information Technology - International Standardized Profiles AMH 3 - Message Handling Systems, 1993
pDISP 12064-1	Information Technology - International Standardized Profiles FOD nnn - ODA - Open Document Format: Image Applications - Simple Document Structure - Raster Graphics Content Architecture, Part 1: FOD 112, Document Applications Profile, August 1993 (balloting ended December 1993)
pDISP 12065-1	Information Technology - International Standardized Profiles ALD 1n - Library and Documentation - Search and Retrieve, Part 1: Specification of ACSE, Presentation, and Session Protocols for Use by Library and Documentation, August 1993
pDISP 12066-1	Information Technology - International Standardized Profiles ALD 2n - Library and Documentation - Interlibrary Loan, Part 1: Generic, August 1993

pDISP 12066-2	Information Technology - International Standardized Profiles ALD 2n - Library and Documentation - Interlibrary Loan, Part 2: Using Connection-Oriented ACSE, August 1993
DIS 12087-1	Image Processing and Interchange (IPI) Standard, Part 1: Common Architecture for Imaging (CAI)
DIS 12087-2	Image Processing and Interchange (IPI) Standard, Part 2: Programmer's Imaging Kernel System (PIKS)
DIS 12087-3	Image Processing and Interchange (IPI) Standard, Part 3: Image Interchange Facility (IIF)
ISO/IEC 12119	Information Technology - Software packages - Quality Requirements and Testing, 1993
ISO/IEC TR 12178	User Requirements for Systems Supporting Time-Critical Communications, December 1993
CD 12227	SQL Ada Module Description Language (SAMeDL)
ISO/IEC TR 12382	Permuted Index of the Vocabulary of Information Technology, 1992
WD 13182	Financial Transactions - Security Architecture - System Overview, TC68/SC6/WG7, 1993
PDTR 13335-1	Information Technology - Security Techniques - Guidelines for Management of Information Technology Security, Part 1: Concepts and Models, SC27/WG1, 1993
WDTR 13335-2	Information Technology - Security Techniques - Guidelines for Management of Information Technology Security, Part 2: Managing and Planning, SC27/WG1, 1993
WDTR 13335-3	Information Technology - Security Techniques - Guidelines for Management of Information Technology Security, Part 3: Techniques, SC27/WG1, 1993
CD 13492	Financial Transactions - Retail Banking Security - Secure Cryptographic Devices, TC68/SC6/WG6, 1993
CD 13522-1	Coding of Multimedia and Hypermedia Information, Part 1: MHEG Objects Representation - Base Notation (ASN.1), 1993 (DIS expected March 1994 and IS in November 1994)
WD 13522-2	Coding of Multimedia and Hypermedia Information, Part 2: Alternate Notation (SMSL), 1993 (CD expected March 1994, DIS in November 1994, and IS in February 1995)
WD 13522-3	Coding of Multimedia and Hypermedia Information, Part 3: MHEG Extensions for Scripting Language Support, 1993 (CD expected December 1994, DIS in June 1995 and IS in December 1995)
CD 13594	Information Technology - Telecommunications and Information Exchange Between Systems - Lower Layers Security Model, 1993 (target date for ITU-TS approval November 1994)
CD 13642	Information Technology - Telecommunications and Information Exchange Between Systems - Specification of the Elements of Management Information Related to OSI Physical Layer Standards, 1993
DIS 13712-1	Information Technology - Open Systems Interconnection - Remote Operations, Part 1: Model, 1993 (X.880) (initiation of ITU-TS ballot approval February 1994) (see 9072-1)
DIS 13712-1 PDAM1	Amendment 1: Built-In Operations, January 1994 [SC21 N 8406]
DIS 13712-2	Information Technology - Open Systems Interconnection - Remote Operations, Part 2: Service, 1993 (X.881) (initiation of ITU-TS ballot approval February 1994) (see 9072-2)
DIS 13712-2 PDAM1	Amendment 1: Mapping to A-UNITDATA and Built-In Operations, January 1994 [SC21 N 8407]
DIS 13712-3	Information Technology - Open Systems Interconnection - Remote Operations, Part 3: Protocol, 1993 (X.882) (initiation of ITU-TS ballot approval February 1994) (see 9072-3)
DIS 13712-3 PDAM1	Amendment 1: Mapping to A-UNITDATA and Built-In Operations, January 1994 [SC21 N 8408]
DIS 13712-4	Information Technology - Open Systems Interconnection - Remote Operations, Part 4: PICS Proforma, 1993 (X.883) (initiation of ITU-TS ballot approval November 1994) (see 9072-4)
WD 13712-5	Information Technology - Open Systems Interconnection - Remote Operations, Part 5: Enhancements, 1993 (initiation of ITU-TS ballot approval June 1995)
DIS 13719-1	Information Technology - Portable Common Tools Environment (PCTE), Part 1: Abstract Specification (ECMA-149), September 1993
DIS 13719-2	Information Technology - Portable Common Tools Environment (PCTE), Part 2: C Programming Language Binding to PCTE (ECMA-158), September 1993
DIS 13719-3	Information Technology - Portable Common Tools Environment (PCTE), Part 3: Ada Programming Language Binding (ECMA-162), September 1993
CD 13818-1	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 1: Systems, SC29/WG11, November 1993 [SC29 N 634] (DIS expected March 1994, IS in November 1994]
CD 13818-2	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 2: Video, SC29/WG11, November 1993 [SC29 N 634] (DIS expected March 1994, IS in November 1994]
CD 13818-3	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 3: Audio, SC29/WG11, November 1993 [SC29 N 635] (DIS expected March 1994, IS in November 1994]
WD 13818-4	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 4: Conformance Testing, SC29/WG11, November 1993 [SC29 N 636] (CD expected November 1994, DIS in March 1995, IS in November 1995]
WD 13818-5	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 5: Technical Report on Software for ISO/IEC 13818, SC29/WG11 (WD expected July 1994, CD in November 1994, DIS in March 1995, IS in November 1995]

WD 13818-6	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 6: System Extensions, SC29/WG11 (WD expected November 1994, CD in March 1995, DIS in November 1995, IS in July 1996]
WD 13818-7	Information Technology - Generic Coding of Moving Pictures and Associated Audio Information, Part 7: Audio Extensions, SC29/WG11 (WD expected November 1996, CD in March 1997, DIS in July 1997, IS in March 1998]

STANDING AND RELATED DOCUMENTS

Standing Documents

SGFS SD-1	Information Technology - International Standardized Profiles - Taxonomy Update, ISP Approval and Maintenance Process, October 1993 [SGFS N 1015]
SGFS SD-3	An Informal Quality Service for Functional Stnadards and the List of Informal Review Experts, August 1993 [SGFS N 977]
SGFS SD-4	Information Technology - Framework and Taxonomy of International Standardized Profiles - Directory of ISPs and Profiles Contained Therein, SGFS N 1049, November 1993
SGFS SD-7	Issues List for Future Development of ISO/IEC TR 10000, SGFS N 1023, September 1993
SC6 SD-4	Directory of ISPs and Profiles Contained Therein, February 1992
SC21 SD-1	Report of the SC21 Secretariat, SC21 Secretariat, January 1993 [JTC1 N 2318]
SC21 SD-2	ISO/IEC JTC1 SC21 Programme of Work (POW) - Target Date Summary for All Active and Published Projects, SC21 Secretariat, October 1993 [SC21 N 8082]
SC21 SD-3	SC21 Inter-Project Dependencies, SC21 Secretariat, May 1992 [SC21 N 6957]
SC21 SD-4	SC21 Strategic Plan, January 1992 [SC21 N 6711]
SC21 SD-5	Rules to be Applied in the SC21 Editing Process, November 1991 [SC21 N 6554]
SC21 SD-6	Directives for the Work of JTC1, Edition 2, 1992
SC21 SD-7	Management Plan for Security, Edition 1, June 1990 [SC21 N 5130]
SC21 SD-8	SC21 Schedule of Meetings, June 1993 [SC21 N 8084]
SC21 SD-9	Approved Commentaries on the Basic Reference Model for Open System Interconnection, OSI Reference Model Editor, November 1991 [SC21 N 6198]
SC21 SD-10	SC21/ITU-TS Collaborative Projects, September 1993 [SC21 N 8083]
SC21 SD-11	Management Guidelines for SC21, December 1993 [SC21 N 8362]

Guidance

SC21 N 7215	Management Guidelines for SC21, June 1992 (to be updated in accordance with SC21 N 8122)
SC21 N 7489	Guide for ITU-TS (CCITT) and ISO/IEC JTC1 Cooperation, December 1992 (Annex K to the ISO/IEC JTC1 Directives, JTC1 N 2119)
SC21 N 8116	Final Steps for the Editing of Standards in the Case of Collaborative Work with ITU-TS, June 1993
SC21 N 8080	Guidelines for Conducting Editing Meetings Using Electronic Mail, June 1993
SC21 N 8132	Identification of Versions in the Foreword of a Standard, June 1993
SC21 N 8024	Programme of Work of ISO/IEC JTC1/SC21/WG1, June 1993

Report to 1994 JTC1 Plenary:

JTC1 N 2707	Proposed Modifications to the ISO/IEC JTC1/SC21 Programme of Work, Secretariat, ISO/IEC JTC1/SC21, November 1993
JTC1 N 2777	Report of JTC1/SC21 to the 1994 JTC1 Plenary Meeting in Washington, DC, Secretariat, ISO/IEC JTC1/SC21, December 1993
JTC1 N 2851	Management Report of JTC1/SC21 to the 1994 JTC1 Plenary Meeting in Washington, DC, Chairman, ISO/IEC JTC1/SC21, January 1994

Reports, Resolutions, and Recommendations from SC21 Plenary Meetings

SC21 N 7978	Rationale for Proposed SC21/WG4 Program Extensions, SC21/WG4, July 1993
SC21 N 7979	Report of the Tenth ISO/IEC JTC1/SC21/WG4 Meeting, Yokohama, 15-24 June 1993, SC21/WG4, September 1993
SC21 N 8021	Report of the ISO/IEC JTC1/SC21/WG1 Meeting, Yokohama, 16-24 June 1993, SC21/WG1, September 1993
SC21 N 8024	ISO/IEC JTC1/SC21/WG1 Programme of Work, SC21/WG1, July 1993
SC21 N 8028	List of Late Contributions and Output Documents of the SC21/WG1 Yokohama Meeting, 16-24 June 1993, SC21/WG1, July 1993
SC21 N 8081	Resolutions of the Ninth Plenary Meeting of ISO/IEC JTC1/SC 21, 29-30 June 1993, Yokohama, Japan, June 1993
SC21 N 8217	Report of the SC21/WG7 Meeting, June 1993, Yokohama, SC21/WG7, September 1993
SC21 N 8027	Resolutions of SC21/WG1, June 1993
SC21 N 8123	Resolutions of SC21/WG3, June 1993
SC21 N 7977	Resolutions of SC21/WG4, June 1993
SC21 N 8055	Resolutions of SC21/WG7, June 1993
SC21 N 8078	Resolutions of SC21/WG8, June 1993
SC21 N 8085	Convenor's Report for SC21/WG1, June 1993
SC21 N 8115	Convenor's Report for SC21/WG3, June 1993

SC21 N 8043	Convenor's Report for SC21/WG4, June 1993
SC21 N 8124	Convenor's Report for SC21/WG7, June 1993
SC21 N 8079	Convenor's Report for SC21/WG8, June 1993

REGIONAL WORKSHOP TECHNICAL REPORTS

EWOS	Guidelines for Managed Object Profiling and Taxonomy, September 1993 (RWS-TR expected February 1994)
EWOS	Framework for Conformance Testing of Network Management Profiles, September 1993 (RWS-TR expected February 1994)
EWOS	Tutorial on FTAM Concurrency Control, November 1993
EWOS	Conformance Testing Vocabulary (EWOS approval expected May 1994)
EWOS	TTCN Style Guide (EWOS approval expected November 1994)
EWOS	Library of Test Specifications (EWOS approval expected November 1994)
EWOS	Guidelines for Managed Object Harmonization (EWOS approval expected November 1994)
OIW	Test Case Selection Rules

JTC1 WORKING DOCUMENTS

JTC1 New Work Item Proposals for SC21

JTC1 N 960	Proposal for an NWI: Management Information Register and Registration Procedure (in June 1993, SC21 recommended to JTC1 that the project be cancelled [SC21 N 7944])
JTC1 N 2246	Proposal for an NWI: Command Sequencer (comments on JTC1 ballot were resolved by SC21 in June 1993 and the revised NWI proposal forwarded to JTC1 for consideration [SC21 N 7943])
JTC1 N 2248	Proposal for an NWI: Enhancement of Directory Operational Security (comments on JTC1 ballot were resolved by SC21 in June 1993 and the revised NWI proposal forwarded to JTC1 for consideration [SC21 N 7933]) (revisions to nine parts of ISO 9594 and possibly one new part; WDs expected February 1994, CDs November 1994, DISs May 1995, and ISs May 1996)
JTC1 N 2249	Proposal for an NWI: Removal of Session Layer Serial Number Limitation (comments on JTC1 ballot were resolved by SC21 in June 1993 and the revised NWI proposal forwarded to JTC1 for consideration [SC21 N 7985])
JTC1 N 2264	Proposal for an NWI: Extensions to ACSE Covering ASOs and ASO-Associations (comments on JTC1 ballot [JTC1 N 2507] were resolved by SC21 by revising the scope of work; the project has been added to SC21 program of work [SC21 N 8076])
JTC1 N 2612	Proposal for an NWI: Open Systems Assessment Methodology, August 1993 (failed to qualify for JTC1 program of work, as five P-members do not commit to active participation [JTC1 N 2773, December 1993])
JTC1 N 2620	Proposal for an NWI: Conformance Testing of OSI Protocols Over OSI Services Provided by Non-OSI Protocols, August 1993 [SC21 N 8011, June 1993] (failed to qualify for JTC1 program of work, as five P-members do not commit to active participation [JTC1 N 2774, December 1993])
JTC1 N 2621	Proposal for an NWI: Conceptual Schema Modelling Facility, August 1993 [SC21 N 8060, June 1993] (balloting ended in November 1993) (WD expected July 1995, CD July 1996, DIS July 1997, and IS July 1998)
JTC1 N 2760	Proposal for an NWI: Amendment to ISO/IEC 8473-1 Covering Extensibility and Quality of Service, December 1993 [SC6 N 8518, November 1993] (balloting ends 16 March 1994) (PDAM to ISO/IEC 8473-1 expected October 1993, DAM March 1994, and AM November 1994)
JTC1 N 2769	Proposal for an NWI: Extension to ISO/IEC 8072 for Protection Quality of Service, December 1993 [SC6 N 8560, November 1993] (balloting ends 1 April 1994)
JTC1 N 2801	Proposal for an NWI: ISO/IEC 7498-n, Architecture for Multipeer Communications [SC21 N 8003] (balloting ends 29 March 1994) (new part to ISO 7498; WD expected in 1995, CD in 1996, DIS in 1997, and IS in 1998)
JTC1 N 2802	Proposal for an NWI: Enhancements to LOTOS, December 1992 [SC21 N 8022] (balloting ends 29 March 1994) (PDAM to ISO 8807 expected June 1995, DAM June 1996, and AM June 1997)
JTC1 N 2803	Proposal for an NWI: Directory Schema Migration, December 1992 [SC21 N 7942] (balloting ends 29 March 1994) (revisions to nine parts of ISO 9594; WDs expected July 1994, CDs November 1994, DISs May 1995, and ISs May 1996)

JTC1—Other

JTC1 N 2642 Rev.	Calling Notice and Draft Agenda for the First Meeting of ISO/IEC JTC1/SC21 Joint Working Group 9, Corrected Version, SC21 Secretariat, September 1993 (to process the interpretation of ISO/IEC Guide 25 for Information Technology Testing Laboratories for Software and Communications Testing Services [JTC1 N 2527] and produce a revision for balloting as a draft technical report; held 30 November to 2 December 1993 in London)
JTC1 N 2775	Summary of Voting on Document JTC1 N 2621, Proposal for a New Work Item: Conceptual Schema Modelling Facility, December 1993
JTC1 N 2835	Report from ISO/IEC JTC1/SC21 Chairman on Activities Related to Application Program Interfaces (APIs) and Modelling Facilities (MFs), January 1994
JTC1 N 2836	JTC1/SC21 Reports on Application Program Interfaces (APIs), January 1994

SGFS WORKING DOCUMENTS

SGFS N 983	UK Discussion Paper Relating to User Requirements Relevant to Open Systems Assessment Methodology, July 1993
SGFS N 1003	Modification of SD-1, SGFS Procedures, for Adoption of PTSs and APIs, August 1993
SGFS N 1043	Liaison Statement to SGFS and EWOS/EG-OSE, OIW, November 1993
SGFS N 1056	EWOS Major Comments on the Third Working Draft of TR 10000 Part 3 (ISO/IEC JTC1/SGFS N 1024) and Proposals for Change, EWOS, November 1993
SGFS N 1065	US Comments on OIW Liaison Statement to SGFS and EWOS/EG-OSE, August 1993
SGFS N 1076	Liaison from AOW/EWOS/OIW to SGFS on Submission of AOM 2x Taxonomy, SGFS, December 1993
SGFS N 1078	Draft Guide to the POSIX Open System Environment (P1003.0/D16.1), IEEE Computer Society, December 1993
SGFS N 1087	Liaison Statement to SC21/SWG-PS, SGFS, December 1993
SGFS N 1089	White Paper on OSE Profiling Concepts, SGFS, December 1993 (materiel offered for integration in ISO/IEC TR 10000)
SGFS N 1090	Liaison Statement to JTC1 on the Subject of PAS and APIs, December 1993
SGFS N 1098	Resolutions Adopted by the SGFS Authorized Subgroup Meeting in Amsterdam, 29 November to 3 December 1993, SGFS, December 1993
SGFS N 1099	Draft Minutes of the SGFS Authorized Subgroup Meeting in Amsterdam, 29 November to 3 December 1993, SGFS, December 1993

SC6 WORKING DOCUMENTS

SC6 N 7951	OSI Lower Layer Security Model, SC6/WG5, 1993
SC6 N 7952	Lower Layer Security Guidelines, SC6/WG5, 1993
SC6 N 8135	Draft Statement of Expected Benefits Regarding Category C Liaison Between the Internet Society and ISO/IEC JTC1/SC6, July 1993
SC6 N 8419	ISO/IEC JTC1/SC6 Liaison Contribution to the Internet Society, November 1993
SC6 N 8420	Statement of Expected Benefits Resulting from Liaison Between ISO/IEC JTC1/SC6 and the Internet Society, November 1993

SC14 WORKING DOCUMENTS

SC14 N 734	Secretariat's Report to ISO/IEC JTC1 Plenary Meeting in Washington, D.C., 1-4 February 1994, SC14 Secretariat, November 1993

SC18 WORKING DOCUMENTS

SC18 N 2233	User Requirements for Security in Text and Office Systems

SC22 WORKING DOCUMENTS

SC22/WG15 N 46 Rev.	Security Interface for POSIX, SC22/WG15, 1993 (approved new work item)

SC27 WORKING DOCUMENTS

SC27 N 209	Non-Repudiation Mechanisms (Part 1: General Model; Part 2: Mechanisms Using Symmetric Key Techniques; and Part 3: Mechanisms Using Asymmetric Techniques), SC27/WG2
SC27 N 467	Collection and Analysis of Requirements for Information Technology Security Criteria, SC27/WG3
SC27 N 685	Security Information Objects, SC27/WG1, 1993
SC27 N 691	Guidelines on the Use and Selection of Security Services and Mechanisms for the Management of Trusted Third Party Services, SC27/WG1, 1993
SC27 N 697	Glossary of Information Technology Security Definitions, SC27/WG1, 1993 (SC27 standing document)
SC27 N 718	Evaluation Criteria for Information Technology Security, Part 2: Introduction and Model, SC27/WG3, 1993
SC27 N 721	Evaluation Criteria for Information Technology Security, Part 3: Functionality of IT Systems, SC27/WG3, 1993
SC27 N 734	Evaluation Criteria for Information Technology Security, Part 1: Assurance of IT Systems, SC27/WG3, 1993
SC27 N 791	Security Incident Reporting; WG1 Meeting No. 7; 12-15 October 1993 in Paris, SC27/WG1, November 1993

SC29 WORKING DOCUMENTS

SC29 N 363	Image Compression Across Multiple Components (WD expected November 1995, CD in November 1996, DIS in July 1997, IS in 1998)
SC29 N 364	Lossy/Lossless Coding of Bi-level Images (WD expected November 1995, CD November 1996, DIS in July 1997, IS in 1998)
SC29 N 365	Compression of Up to 5-D Images (WD expected November 1995, CD in November 1996, DIS in July 1997, in IS 1998)
SC29 N 366	Lossless Compression of Continuous-Tone Still Pictures (WD expected November 1995, CD in November 1996, DIS in July 1997, IS in 1998)
SC29 N 367	Very-low Bitrate Audio-Visual Coding (in four parts: Systems, Video, Audio, and Conformance Testing; WD expected in November 1996, CD in November 1997, DIS in March 1998, and IS in November 1998)

SC29 N 368	Low-Bit-Rate Audio Coding (WD expected in November 1995 and CD in November 1997)

SC21 WORKING DOCUMENTS

SC21 N 197	Concepts and Terminology for the Conceptual Schema and the Information Base, TC97/SC5, March 1982
SC21 N 236	Assessment Guidelines for Conceptual Schema Language Proposals, TC97/SC21/WG5-3, August 1985
SC21 N 3283	Working Draft for Lower-Layer Security Model, December 1988 [SC21/WG1]
SC21 N 3711	Requirements for Multipeer Data Transmission, July 1989
SC21 N 3885	UN/EDIFACT Information Pack, September 1989
SC21 N 3906	Final Report to SC21 in Florence on the Reassessment of Project JTC 1.21.9.1 on Multipeer Data Transmission, October 1989
SC21 N 4077	Fault Management Working Document, SC21/WG4, December 1989
SC21 N 4085	Accounting Management Working Document, Third Version, SC21/WG4, November 1989
SC21 N 4091	OSI Security Management Working Document, November 1989
SC21 N 4189	Comments on the Integration of X-Windows into the OSI Environment, December 1989
SC21 N 4279	CCR Conformance Test Suite, January 1990 (new work item) (CD text expected June 1995)
SC21 N 4681	User Requirements for Multi-Party Communications (MPC), Canada, May 1990
SC21 N 4833	Report to JTC1 from SC27 on Security Techniques, SC27 Secretariat, May 1990 [SC27 N 94]
SC21 N 4835	Report of the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990, SC27 Secretariat, May 1990 [SC27 N 92]
SC21 N 4836	Resolutions Taken at the First Plenary Meeting of SC27 at Stockholm, 24-26 April 1990, May 1990 [SC27 N 94]
SC21 N 4970	Systems Management Tutorial - Annex A: Access Control, May 1990
SC21 N 5110	Call to National Bodies and Liaison Organizations for Contributions on Technical Structure of Quality of Service (QOS) Architecture, May 1990
SC21 N 5137	Data Management Export/Import for SQL and IRDS, SC21/WG3, October 1990 (new work item; CD text expected December 1992)
SC21 N 5165	FTAM Constraint Set and Document Types for CGM, SC21/WG5, June 1990
SC21 N 5194	Resolutions of the Fourth Plenary Meeting of SC21, June 1990, Seoul, SC21, June 1990
SC21 N 5228	Report of the ISO/IEC JTC1/SC21 Plenary Meeting, June 1990, Seoul, Korea, July 1990
SC21 N 5229	Report of the JTC1/SC21 Plenary Meeting, June 1990, Seoul, Republic of Korea
SC21 N 5394	Collections of Definitions of OSI Vocabulary, June 1991
SC21 N 5580	New Area of Work for SC27/WG1 on IT Security Information Objects, January 1991
SC21 N 5581	New Area of Work for SC27/WG1 on IT Security Terminology, January 1991
SC21 N 5593	The Role of the Extended Application Layer Structure in the Standardization of RPC, ECMA, January 1991
SC21 N 5635	Report of the Special Working Group on a Conceptual Model for Electronic Data Interchange Standards and Services (SWG-EDI), January 1991
SC21 N 5714	Resolutions of the ISO/IEC JTC1 Advisory Group Meeting, Washington, DC, 19-21 February 1991, March 1991
SC21 N 5731	Progression of the Upper Layers Security Standards, Canada, April 1991
SC21 N 5758	Discussion Paper on Conformance and Registration, BSI, March 1991
SC21 N 5817	Binding Concepts Within RPC, ECMA, March 1991
SC21 N 5819	Modelling Rationale for OSI RPC, ECMA, March 1991
SC21 N 6017	Comments on Standardization of Application Programmatic (sic) Interfaces, WG4, May 1991
SC21 N 6037	Need for Security Services with OSI Management, SG4, July 1991
SC21 N 6069	Proposed New WG6 Question Q6/2 on the Relationship Between the OSI Upper Layer Architecture and ODP, July 1991
SC21 N 6070	Working Draft Answer to the Proposed WG6 Question on the Architectural Relationship Between OSI and ODP, June 1991
SC21 N 6086	Resolution of Ballot Comments on the NP on ODP Trader, SC21/WG7, May 1991
SC21 N 6088	Proposal for a WG7 Question on the Suitability of the Formal Description Technique Z for Use in ODP, May 1991
SC21 N 6110	Session Layer Extension to Support Re-Use of Transport Connections, WG6, JTC1 N 1436, July 1991 (voting ended 21 October 1991) (new work item)
SC21 N 6130	Working Draft for ASN.1 Encoding Rules to Provide Upper Layer Security and Compression, WG6, June 1991
SC21 N 6157	Answer to CCITT SG VII Q 23 on OSI Reference Model Regarding ISDN, May 1991
SC21 N 6158	Final Answer to Q1/62 (Quality of Service Architectural Issues), WG1, May 1991
SC21 N 6159	Framework on Quality of Service, WG1, May 1991 (new project proposal for a TR) (PDTR projected for May 1993, DTR May 1994, TR May 1995)
SC21 N 6160	Catalogue of PICS Proforma Notations, WG1, July 1991
SC21 N 6194	Final Answer to Q1/63.1--Meaning of Conformance to Objects in the Context of OSI Management, WG1, May 1991

SC21 N 6197	WG1 Position on the Reactivation of Project 1.21.9.1 (Multi-Peer Data Transmission), WG1, July 1991 (national body comments requested by 31 March 1992)
SC21 N 6198	Approved Commentaries on the OSI Basic Reference Model [SC21 SD-9], July 1991
SC21 N 6224	Proposed EDIFACT/FTAM Document Type, WG5, July 1991
SC21 N 6225	Response to Liaison from JTC1/SC24/WG3 about CGM Document Types, July 1991
SC21 N 6227	Virtual Terminal Support of ODA, WG5, July 1991
SC21 N 6249	Resolutions of the SC21/WG3 Meeting, Arles (May 1991), July 1991
SC21 N 6251	Proposed New Question on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM), July 1991
SC21 N 6252	Revision of the IRDS Framework, WG3, July 1991 (new work item)
SC21 N 6253	Proposed New Question on the Approach to Remote IRDS Access, July 1991
SC21 N 6257	Recommendation on NWI for Stored DBL Procedures, July 1991
SC21 N 6273	Resolutions of the Seventh Plenary Meeting of ISO/IEC JTC1/SC21, 4-5 June 1991, Arles, France, June 1991
SC21 N 6306	[Information Technology - Open Systems Interconnection - Systems Management -] Performance Management Working Document - Seventh Draft, July 1991
SC21 N 6370	Register of Object Identifier Components Allocated to Areas of Joint ISO/CCITT Work, August 1991
SC21 N 6403	Proposal for a New Work Item: Generic Operating System Interface, September 1991
SC21 N 6478	Target Dates for Completion of SC22 Projects, November 1991
SC21 N 6527	Resolutions of the ISO/IEC JTC1 Plenary Meeting, October 2-4, 1991, Madrid, JTC1 Secretariat
SC21 N 6530	Report of the JTC1 Plenary Ad Hoc Group on EDI, October 1991
SC21 N 6586	Meeting Report - Collaborative CCITT Q19/VII and SC21/WG6 Meeting on Upper Layers Security, December 1991
SC21 N 6604	Summary of Voting on Document JTC 1 N 1434, Proposal for a New Work Item on Enhancements to Light Weight Encoding Rules, JTC1 Secretariat, April 1992
SC21 N 6606	Collection of Liaison Statements from SC27 to SC21, May 1992
SC21 N 6614	SC21 Recommended Action to Address Problems of Data Modelling Standards Coordination, December 1991
SC21 N 6615	The Processing of Standards in SC21, SC21 Special Meeting on Structure and Organization, ANSI, 10-13 December 1991, December 1991
SC21 N 6619	Resolutions of the SC21 Special Meeting on Structure and Organization, ANSI, 10-13 December 1991, December 1991
SC21 N 6638	Issues for National Body and Liaison Organization Comment on RPC, June 1992
SC21 N 6639	Proposed Liaison Statement to SC21/WG4 Regarding General and Dependent Conformance, January 1992
SC21 N 6640	Health Warning Regarding General and Dependent Conformance, JTC1-CCITT Interim Meeting on Conformance, November 1991, January 1992
SC21 N 6653	Various Contributions to the ISO/IEC JTC1/SC21 Special Group Meeting on Conceptual Schema and Common Data Modelling Facilities, 9-13 March 1992, Renesse, The Netherlands
SC21 N 6656	Liaison Statement to SC21/WG6 on Compatibility of ROS and RPC
SC21 N 6664	Liaison Statement to SC22/WG15 on Software Management, January 1992
SC21 N 6667	Contributions from ISO/IEC JTC1/SC18 Regarding the Progression of Work on Multimedia and Hypermedia Model/Framework
SC21 N 6695	Liaison Statement from SC21/WG1 Security Ad Hoc Group to SC21/WG5 TP on Preliminary Security Model, January 1992
SC21 N 6711	SC21 SD-4, SC21 Strategic Plan, January 1992
SC21 N 6713	CCITT Circular No. 118 Regarding the Catalogue of CCITT Recommendations, January 1992
SC21 N 6714	List of Contact Points of SIGs/EGs of Regional Workshops, January 1992
SC21 N 6715	Letter from ITTF/CCITT Regarding Preparation of CCITT-ISO/IEC Common Text, January 1992
SC21 N 6719	Recommendations of the CCITT and ISO Collaborative Interim Meeting Covering ROSE Enhancements, April 1992
SC21 N 6722	Issues Concerning Mapping of ROSE APDUs onto A-UNIT-DATA, January 1992
SC21 N 6723	Enhancement to ROSE, Part 3: Concepts, Model and Notation, Working Draft, January 1992 (IS expected November 1993)
SC21 N 6724	Enhancement to ROSE, Part 1: Service Definition, Working Draft, January 1992 (IS expected November 1993)
SC21 N 6725	Enhancement to ROSE, Protocol Definition, Working Draft, January 1992 (IS expected November 1993)
SC21 N 6728	Summary of Planned Contributions to the Renesse Special Meeting on Conceptual Schema Facilities and Common Data Modelling Facilities, April 1992
SC21 N 6737	Object Oriented Task Group Final Report, February 1992
SC21 N 6749	Proposal for a New Work Item on Information Technology - Text Communication - Coordinated Time Service in an OSI Environment, February 1992

SC21 N 6755	Contribution on Key Management, February 1992
SC21 N 6756	TP/CCR One-Phase Commitment, February 1992
SC21 N 6759	Recommendation on SQL2 Progression (ISO/IEC DIS 9075), February 1992
SC21 N 6760	Minutes of the SQL2 Editing Meeting, Kawagoe, February 1992
SC21 N 6765	Guide to Open Systems Security Collaborative SC21/CCITT Security Ad Hoc Group Meeting, November 1991, February 1992
SC21 N 6776	Framework & Taxonomy of International Standardized Profiles - Directory of ISPs and Profiles Contained Therein, March 1992
SC21 N 6777	Letter from ISO Regarding the Disbandment of GOST, March 1992
SC21 N 6778	CCITT Interim Meeting Schedule - Late 1992/Early 1993, March 1992
SC21 N 6779	Statement Regarding Participation at CCITT Study Group Meetings, March 1992
SC21 N 6793	Proposed Mechanism for Soliciting National Body Input on Multipeer/Multicast Application Requirements, March 1992
SC21 N 6794	Preliminary Requirements for a Multi-peer Data Communication Architecture, March 1992
SC21 N 6796	US Response on Application Context Negotiation, March 1992
SC21 N 6797	Comments on SC21 N 6068, Modelling Recovery in the Application Layer, March 1992
SC21 N 6798	US Request for Extensions to ACSE, March 1992
SC21 N 6799	Contribution on Upper Layer Management, March 1992
SC21 N 6801	Comments on SC21 Recommended Action to Address Problems of Data Modelling Standards Coordination, March 1992
SC21 N 6802	Problems with Certifying FTAM Implementation as Conformant, March 1992
SC21 N 6807	Protocol Version Numbers, March 1992
SC21 N 6808	Organization of Work on OSI and ODP Architecture, UK National Body, March 1992
SC21 N 6809	Request for Reassessment of the Terminal Management Project, March 1992
SC21 N 6810	UK Position on General and Dependent Conformance, March 1992
SC21 N 6811	FTAM Aspects of Security, March 1992
SC21 N 6812	Request to Apply the Procedures for the Reactivation of the Multi-Peer Data Transmission Project (MPDT), March 1992
SC21 N 6813	Draft Addendum for Multi-Peer Data Transmission Project (MPDT), March 1992
SC21 N 6814	Liaison Statement to SC21 on Lower Layer Multicast Work SC6 Enhanced Transport Mechanisms Meeting, March 1992
SC21 N 6819	Report of the ISO/IEC-CCITT Joint OSI Conformance Group Interim Meeting Held in Durham, North Carolina, 4-8 November 1991, March 1992
SC21 N 6820	Liaison Statement for SC22/WG11, Binding Techniques, to SC21/WG6 RPC Rapporteur Group, March 1992
SC21 N 6821	Internationalization of the Directory, January 1992
SC21 N 6822	UK Response to N 6011, Call for Contributions on Directory Enhancements, January 1992
SC21 N 6842	US Concerns Regarding the Ballot Responses on the Authentication Service NP and Enhancements to Directory Authentication NP, April 1992
SC21 N 6843	Contribution on Non-Repudiation Framework, April 1992
SC21 N 6844	Contribution on Security Frameworks Overview, April 1992
SC21 N 6870	Proposal for a New Work Item on Mapping of the OSI System Management - Object Management Function onto Message Oriented Text Interchange System (MOTIS), April 1992
SC21 N 6872	Liaison Statement to CCITT Q20/VII and SC21/WG4 from SC18 on MHS Use of Directory, April 1992
SC21 N 6875	Liaison Statement to SC21 from SC18 on Revised Draft Guide to Open Systems Security, April 1992
SC21 N 6877	Liaison Statement to SC21 from SC18 on Security Framework SC18, April 1992
SC21 N 6878	Liaison Statement to CCITT Q19/VII and SC21/WG6 from SC18 on Use of the Security Exchange ASE, April 1992
SC21 N 6879	Liaison Statement to SC21/WG6 FTAM from SC18 on MHS File Transfer Body Part Type, April 1992
SC21 N 6880	Liaison Statement to CCITT Q19/VII and SC21/WG6 from SC18 on Reliable Transfer Service Element (RTSE), April 1992
SC21 N 6881	Liaison Statement to SC21/WG1 from SC18 on Conformance in Response to SC18 N 3291, April 1992
SC21 N 6883	Report of the Secretariat to the SC21 Meeting in Ottawa, 2-3 June 1992, April 1992
SC21 N 6891	Liaison Statement to SC18 and SC21 on the Status of CCITT X.400/X.500 PICS Proforma Recommendations and Future Collaborative Work, May 1992
SC21 N 6892	Liaison Statement to SC21/WG4 on Atomic Transaction Interfaces, May 1992
SC21 N 6893	Liaison Statement to SC21 on Approval of Management Framework, May 1992
SC21 N 6894	Liaison Statement to Joint CCITT/ISO 9596-2/X.712 Editing Meeting, 29 May 1992, Ottawa, May 1992

SC21 N 6896	Liaison Statement to Joint CCITT/ISO 10164-13/X.738 Editing Meeting, 29 May to 3 June 1992, Ottawa, May 1992
SC21 N 6897	Liaison Statement to SC6 and SC21 on Consumer Network, May 1992
SC21 N 6902	Liaison Statement to SC21 on Revision of the OSI Reference Model, May 1992
SC21 N 6903	Request for the Work on Procedures for the Operation of Registration Authorities: Application Processes and Application Entities to Become Collaborative, May 1992
SC21 N 6904	Liaison Statement to SC21 on Mapping of ROSE APDUs onto the A-UNIT-DATA Service, May 1992
SC21 N 6905	Liaison Statement to SC21/WG6: Report on Q26/VII Meeting, April 1992, May 1992
SC21 N 6906	Liaison Statement to SC21 on Efficiency of OSI Protocols, May 1992
SC21 N 6907	Liaison Statement to SC21 Concerning Collaborative Work on ODP, Security, ASN.1, ROSE, and RTSE, May 1992
SC21 N 6914	Liaison Statement to SC21: Request for Review & Comment on Profile Choices for Subclasses of the EFD/LOG Managed Object Classes Using Allomorphism & Best Efforts Management, May 1992
SC21 N 6915	Liaison Statement to SC21 Regarding Profiles for Systems Management Functions (10164-1 to -6) & Definition of Management Information (10165-2), May 1992
SC21 N 6916	Liaison Statement to SC21/WG6 Concerning the Use of ASN.1 in the Image Processing and Interchange Image Interchange Facility (IPI-IIF) Standard, May 1992
SC21 N 6929	JTC1 National Body Comments Received on JTC1 N 1756, Request for Review and Comment on the SC21 Recommended Action to Address Problems of Data Modelling Standards Coordination, May 1992
SC21 N 6931	Working Draft for SQL-3, Interim Database Languages Meeting, Japan, May 1992
SC21 N 6943	Requirements and Recommendations Regarding Protocol Version Numbers, May 1992
SC21 N 6943 Rev	Requirements and Proposed Recommendations of the Protocol Version Numbers Pre-Meeting (and the Initial ITTF Response), August 1992, Revised
SC21 N 6945	Recommendations and Proposed Work on Conceptual Schema and Data Modelling Facilities, May 1992
SC21 N 6948	Responses to the Proposed Mechanism for Soliciting National Body Input on Multipeer/Multicast Application Requirements, May 1992
SC21 N 6951	Reference Material on Conceptual Schema and Common Data Modelling Facilities, May 1992
SC21 N 6952	Report of the 9-13 March 1992 Renesse Meeting of the SC21 Special Group on Conceptual Schema and Common Data Modelling Facilities, May 1992
SC21 N 6955	Stocktaking of Standards and Standards Projects which Make Use of a Data Modelling Facility or of a Conceptual Schema, May 1992
SC21 N 6956	Status Report on CCITT SG Activities, May 1992
SC21 N 6957	Project Dependencies, June 1992
SC21 N 6961	SC21/WG1 Decision on MPDT Reactivation, May 1992
SC21 N 6966	Incorporation of Versions and Extensibility Technical Material into Existing Standards and Other Documents, May 1992
SC21 N 6967	Modelling Recovery in the Application Layer, May 1992
SC21 N 6968	Request for Comment on Issues Concerning Upper Layer Management, May 1992
SC21 N 6969	Comments on SC21 N 6943, Recommendations and Requirements on Protocol Version Numbers, May 1992
SC21 N 6970	Call for Comments on the Progression of the ALS Extension to Cover Connectionless Mode of Communications, May 1992
SC21 N 6971	Application of XALS Concepts to Specification of Mappings, May 1992
SC21 N 6972	Draft Answer to Q6/2 - Relationship Between the OSI Upper Layer Architecture and ODP, May 1992
SC21 N 6974	Liaison Statement to SC6 Concerning a Request for Incorporation of New Protocol Information Attributes in ISO/IEC 9594-6/DAM 1, June 1992
SC21 N 6975	Need for Procedures to Coordinate the Definition and Extension of Directory Objects, May 1992
SC21 N 6983	Liaison Statement to SC24 Concerning the Use of ASN.1 in the IPI/IIF Standards, May 1992
SC21 N 6984	Class of Mappings from a Single ASN.1 Type to an FTAM Document Type, July 1992 (target dates are WD in July 1993, CD in July 1994, DIS in July 1995, and IS in July 1996)
SC21 N 6985	Request for Comments on Compression in Presentation Layer, June 1992
SC21 N 6992	Generic Upper Layer Security (GULS), Part 1: Overview, Models and Notation, Third Working Draft, May 1992 (SC21/WG6)
SC21 N 6993	Generic Upper Layer Security (GULS), Part 2: SESE Service Definition, Third Working Draft, May 1992 (SC21/WG6)
SC21 N 6994	Generic Upper Layer Security (GULS), Part 3: SESE Protocol Specification Third Working Draft, May 1992 (SC21/WG6)
SC21 N 6995	Generic Upper Layer Security (GULS), Part 4: Protecting Transfer Syntax Specification, Third Working Draft, May 1992 (SC21/WG6)
SC21 N 6996	Liaison Statement to SC6 on Common Aspects of OSI Upper/Lower Layer Security Standards, May 1992
SC21 N 6997	Liaison Statement to ECMA on Security in the Upper Layers, May 1992

SC21 N 6998	Authentication and Related Security Services for Distributed Applications, July 1992 [target dates: WD (5/93), CD (5/94), DIS (5/95), and IS (9/96)]
SC21 N 7011	Liaison Statement to SC18 on Compatibility of ROSE and RPC SC21/WG6, May 1992
SC21 N 7013	Enhancement to ROSE Concepts, Model and Notation, ROSE Service Definition and Protocol Specification, July 1992 [addendum or addenda to ISO 9072-1, ISO 9072-2, and ISO 9072-3; target dates are WD#1 (5/92), WD#2 (11/92), CD (8/93), DIS (2/94), and IS (2/95)]
SC21 N 7014	ACSE Enhancements Covering ASOs and ASO-associations
SC21 N 7016	Presentation Connection-Oriented Abstract Test Suite (ATS), Specific Partial ATS
SC21 N 7018	Use of Systems Management for Administration of the Directory [JTC1 N 1440R]
SC21 N 7020	Enhancement of Directory Operational Security, July 1992 [would result in an addenda to ISO 9594-1 through ISO 9594-9 and possibly one new part; target dates are: WD (11/94), CD (10/95), DAM (10/96), and IS (10/97)]
SC21 N 7021	Registration of Question Q4/4 on Directory Schema Migration, Including Disposition of Comments, May 1992
SC21 N 7024	Request for Contributions on Use of Systems Management for Administration of the Directory, May 1992
SC21 N 7025	Request for Contributions on Movement of Directory Information by Means Other Than Directory Protocols, May 1992
SC21 N 7026	Request for Comments on the Need for an Extension to the Directory Standard to Support Extended Relationships Among Directory Entries, May 1992
SC21 N 7028	Status of Directory Defects, May 1992
SC21 N 7042	The RM-ODP and Standardization of APIs, May 1992
SC21 N 7047	ODP Trader, July 1992, WG7, WD status (CD expected November 1993; DIS November 1994; IS November 1995)
SC21 N 7051	Proposed Draft Answer to Question Q7/1 on the Suitability of the Formal Description Z for Use in ODP, May 1992
SC21 N 7052	Editing Instructions for a Technical Report on Use of FDTs (Specification Technique) in ODP, May 1992, WG7, WD status (PDTR expected July 1994)
SC21 N 7057	List of Open and Resolved Issues, SC21/WG7, May 1992
SC21 N 7062	Liaison Statement to SC6 on Multipeer Data Transmission, May 1992
SC21 N 7063	Liaison Statement to CCITT SG VII on Multipeer Data Transmission, May 1992
SC21 N 7066	Liaison Statement to SC6 Concerning Quality of Service (QOS), ISO/IEC JTC1/SC21 Meeting, Ottawa, June 1992, July 1992
SC21 N 7067	Results of the SC21/WG1 Meeting on Quality of Service (QOS) Framework, May 1992 (CD expected June 1993; DIS June 1994; IS June 1995)
SC21 N 7069	Draft Answer to Q1/49.9 on Long-term Solution to General and Dependent Conformance, ISO/IEC JTC1/SC21/WG1 Meeting, Ottawa, May 1992, July 1992
SC21 N 7073	Proposed New Sub-Question Q1/49.9 on Long-term Solution to General and Dependent Conformance, ISO/IEC JTC1/SC21/WG1 Meeting, Ottawa, in May 1992, July 1992
SC21 N 7074	Liaison Statement to JTC1/SGFS on Conformance Testing, May 1992
SC21 N 7075	Liaison Statement to SC6 on ICS Proforma, May 1992
SC21 N 7076	Liaison Statement to SC18 on Conformance Testing, May 1992
SC21 N 7078	Draft Answer to Q1/49.8 - Conformance and Registration, May 1992
SC21 N 7079	Working Draft Answer to Q1/63.2 - Testability of Managed Objects, May 1992
SC21 N 7080	Liaison Statements to EWOS on Conformance Testing, May 1992
SC21 N 7086	Liaison Statement to SC18 on Security, May 1992
SC21 N 7087	Liaison Statement to SC27 on Security, May 1992
SC21 N 7088	Proposed New Question Q1/66 on ODP Conformance Testing Methodology, May 1992
SC21 N 7089	Statement on Scope and Usability of the Open Systems Security Framework, May 1992
SC21 N 7090	Proposed New Question Q1/65 on User Requirements for OSI Systems Supporting Time Critical Communications, May 1992
SC21 N 7091	Liaison Statements to SC18 on Quality of Service, May 1992
SC21 N 7092	Proposed New Question Q1/67 on Generalization of ASO Concepts, May 1992
SC21 N 7093	Proposed New Question Q1/68 on the Definition of the Term Application-Process-Title in the OSI Reference Model, May 1992
SC21 N 7094	Draft Answer to Q1/68 - Definition of the Term Application-Process-Title in the OSI Reference Model, May 1992
SC21 N 7096	Draft Answer to Q1/48.6 - G-LOTOS, May 1992
SC21 N 7098	Proposed New Question Q1/69 on Conformance Assessments for OSI Security, May 1992
SC21 N 7099	Resolutions Approved by SC21/WG1 at Its Ottawa Meeting, 20-28 May 1992, May 1992
SC21 N 7101	List of Late Input Documents and Output Documents of the SC21/WG1 Ottawa Meeting, May 1992
SC21 N 7102	Extensions to ISO/IEC 9594-8 (Certificate Definitions)
SC21 N 7105	Reply and Disposition of Comments on NP on Development of Enhanced Functionality for CMIS/P (JTC1 N 1667), ISO/IEC JTC1/SC21/WG4 Meeting, Ottawa, May 1992, August 1992

SC21 N 7106	Agreed Requirements for Enhanced Functionality for SM Communications (JTC1 N 1439), May 1992
SC21 N 7107	Disposition of Ballot Comments on JTC1 N 1439, Proposal for a NP on Enhanced Event Handling & Log Control (JTC1 N 1439), May 1992
SC21 N 7109	Command Sequencer for Systems Management, July 1992
SC21 N 7116	Working Document on Complex Attribute Types, July 1992
SC21 N 7117	Request for National Body Input on Principles of Conformance for Managing Systems, July 1992
SC21 N 7118	Management Domains Architecture, WG4, July 1992 (part of the Extended Systems Management Architecture)
SC21 N 7119	Management Domain Management Function, WG4, June 1992
SC21 N 7122	Working Draft on Application Context for Systems Management with TP (CD expected December 1992; DIS February 1994; IS February 1995)
SC21 N 7126	General Relationship Model–Third Working Draft, WG4, May 1992
SC21 N 7129	Request for National Body Contributions to Progress Work on Distributed Management, May 1992
SC21 N 7131	Request for National Body Input Regarding Definition of Common Terms and Use of Formal Description Techniques in SMI Standards, May 1992
SC21 N 7132	Request for National Body Comment on NWI for Library/Catalogue, July 1992
SC21 N 7133	Coherence of Extended Management Architecture, May 1992
SC21 N 7134	Preliminary Document on Multiple Input Metric Object, May 1992
SC21 N 7135	Call for Contributions on Priority Mechanisms in Systems Management, May 1992
SC21 N 7140	Reply to Liaison Statement for CCITT SG VII Regarding the Comments on Notational Tools in SC21 N 6568, July 1992
SC21 N 7143	Comments on Document SC21 N 6897 from CCITT Q9/VII on Customer Network Management, May 1992
SC21 N 7144	Liaison Statement to SC18 Concerning Mapping of Systems Management Object Management Function onto MOTIS, May 1992
SC21 N 7145	Liaison Statement to SC21/WG1, SC21/WG6 (8), SC6 and SC27 on Security Requirements for Systems Management, May 1992
SC21 N 7146	Liaison Statement to SC22/WG15 on Software Management, May 1992
SC21 N 7147	Liaison Statement to CCITT Q23/IV on Software MO, May 1992
SC21 N 7148	Response to the SC6 Liaison Statement on Event Definition, May 1992
SC21 N 7149	Liaison Statement to SC18 Regarding the Status of the Security Exchange Work, May 1992
SC21 N 7156	Proposed NP for Transaction Processing Abstract Test Suites, July 1992 [part of the TP Conformance Testing Standard; target dates are WD (10/93), CD (6/94), DIS (6/95), and IS (6/96)]
SC21 N 7160	FTAM Security Issues, 29 May 1992
SC21 N 7162	Status of Project JTC1.21.12.08.02, FTAM Virtual Filestore Service Enhancements, June 1992
SC21 N 7165	TP Commitment Optimization Issues and Resolutions, May 1992
SC21 N 7166	Requirements and Issues for the Separation of Data and Commitment Flows in OSI TP, May 1992
SC21 N 7167	Request for Contributions on OSI TP Subtransactions, May 1992
SC21 N 7168	Request for Comments on Issues Concerning TP Association Pool Management, May 1992
SC21 N 7171	Revised TP Test Suite Structure and Test Purposes, Working Draft, WG5, May 1992 (CD expected June 1993; DIS June 1994; IS June 1995)
SC21 N 7172	General Principles for the Development of TP Test Cases, May 1992
SC21 N 7173	Open Issues and Questions for the Development of TP Test Cases, May 1992
SC21 N 7175	Liaison Statement to SC6 on Requirement for Non-Blocking Transport Expedited Service, May 1992
SC21 N 7177	Proposed New Work Item for Remote Database Access (RDA), Part 3: IRDS Specialization, Ottawa, May 1992
SC21 N 7178	Proposed NP for Guidelines for the Design of IRDS Content Modules, July 1992 (technical report; target dates are WD (6/93), CD (6/94), DIS (6/95), and IS (6/96)]
SC21 N 7179	SQL Multimedia and Application Packages (SQL/MM), NWI Proposal, December 1992
SC21 N 7180	Proposed Draft Answer to Question Q3/001 - Object Database, May 1992
SC21 N 7181	Proposed Draft Answer to Question Q3/009 - Remote IRDS Access, May 1992
SC21 N 7182	Liaison Statement to ECMA TC33 on IRDS/PCTE, May 1992
SC21 N 7183	Liaison Statement to EWOS/EG DBE on Profiling SQL/RDA, May 1992
SC21 N 7184	Liaison Statement to JTC1/WG3 on EDI, May 1992
SC21 N 7185	Liaison Statement to JTC1/SC14 on Data Elements, May 1992
SC21 N 7186	Liaison Statement to SC18 on Full-Text Manipulation, May 1992
SC21 N 7191	Liaison Statement to ISO TC184/SC5 on Reference Model and IRDS for Automation, May 1992
SC21 N 7195	SC21 Position on SC21 N 6484 Guide for CCITT and JTC1 Collaboration, June 1992
SC21 N 7196	SC21 SD- 8, SC21 Schedule of Meetings SC21 Plenary Meeting, June 1992, Ottawa, June 1992
SC21 N 7197	Response to the Request from SGFS for Comments on Issues Regarding Registration and ISPs, March 1992

SC21 N 7199	Remote Database Access (RDA), ISO 9579, Part 3: IRDS Specialization, July 1992 [target dates are WD (7/94), CD (7/95), DIS (7/96), and IS (7/97)]
SC21 N 7201	Amendment to ISO 10728 for C Language Binding, August 1992
SC21 N 7203	IRDS Framework Revision
SC21 N 7204 Rev	Resolutions of the Eight Plenary Meeting of ISO/IEC JTC1/SC21, 2-3 June 1992, Ottawa, Canada, June 1992
SC21 N 7205	ISO/IEC JTC1/SC21 Programme of Work, September 1992
SC21 N 7208	Proposal for an SC21 SWG on Modelling Facilities (see also SC21 N 6945), June 1992
SC21 N 7209	Initial SC21 Considerations in Support of the Initiation of a Study Period on Application Programmatic Interfaces, June 1992
SC21 N 7214	Rapporteur's Report on SC21 Strategic Planning, June 1992
SC21 N 7215	Revised Management Guidelines for ISO/IEC JTC1/SC21, June 1992
SC21 N 7218	Table of Replies for ISO/IEC 9545/DAM 1, Information Technology Open Systems Interconnection - Application Layer Structure, Amendment 1: Extended Application Layer Structure, June 1992
SC21 N 7268	Collection of Definitions of OSI Vocabulary (June 1992 version), July 1992
SC21 N 7292	Guide for Open Systems Security, August 1992 [SC21/WG1]
SC21 N 7335	Working Draft for LOTOS Description of the CCR Protocol, August 1992 (CD expected December 1992; DIS June 1993; IS June 1994)
SC21 N 7336	Working Draft for LOTOS Description of the CCR Service, August 1992 (CD expected December 1992; DIS June 1993; IS June 1994)
SC21 N 7360	Development of the SGFS Procedures to Cover Other TCs and the Open System En...onment (SGFS N 590), September 1992
SC21 N 7375	Call for Contributions on SC21/WG4 Title and Terms of Reference, October 1992
SC21 N 7379	Liaison Statement to SC21 on OSI Profile Conformance Requirements in TR 10000-1, October 1992
SC21 N 7392	US Contribution to the SC21 Special Working Group Meeting on Modelling Facilities, 7-11 December 1992 in Namur, Belgium, October 1992
SC21 N 7417	Association Management Concepts, November 1992
SC21 N 7425	Draft First Report on the New Work Area on Programmatic Interfaces, November 1992
SC21 N 7430	Working Draft of the Technical Report on Multimedia and Hypermedia: Model and Framework, Version 1, October 1992
SC21 N 7483	Proposal for a New Work Item on Mapping of OSI System Management - Object Management Function onto Message Handling Service (MHS), December 1992 (WD expected in June 1993, CD in November 1993, DIS in June 1994, and IS in June 1995)
SC21 N 7486	Draft IRDS Conceptual Schema, December 1992
SC21 N 7566	Directory Implementor's Guide, Version 7, January 1993
SC21 N 7625	Status of Work on the Separation of Data and Commit Flows in OSI-TP, February 1993
SC21 N 7626	Request for Contributions for OSI-TP Subtransactions, February 1993
SC21 N 7644	TP Commitment Optimizations - Topics and Their Resolution, February 1993
SC21 N 7672	Revised Working Draft for TP Test Suite Structure, March 1993
SC21 N 7676	Initial Abstract Test Suite for TP, March 1993
SC21 N 7713	Resolutions of the ISO/IEC JTC1 Plenary Meeting, 23-26 March 1993, Berlin, Germany, April 1993
SC21 N 7720	Revised Title and Scope for SC21, April 1993
SC21 N 7728	Proposals for Re-assessment or Cancellation of Specific SC21 Projects, April 1993
SC21 N 7747	Revised Text of the Guide for CCITT and ISO/IEC JTC1 Cooperation, April 1993
SC21 N 7749	The International Telecommunication Union - An Overview, April 1993
SC21 N 7817	Requirement for Timely Progression of the Application Guidelines, May 1993
SC21 N 7841	Report of the Ninth Plenary Meeting of ISO/IEC JTC1/SC 21 to be held from 29-30 June 1993 in Yokohama, Japan, May 1993
SC21 N 7902	Methodology and Guidelines for the Development of Application Layer Standards, June 1993
SC21 N 7914	Working Document on Authentication and Related Security Services, August 1993 (four parts are planned: Introduction and Model; Generic Abstract Security Service; Specific Security Service Definitions; and Protocol Specifications) (CD expected December 1994, DIS December 1995, and IS December 1996)
SC21 N 7915	Liaison Statement to SC6 in Reply to SC6 N 7961 and 7614, SC21/WG8, August 1993
SC21 N 7930	Working Document on Use of OSI Systems Management for the Administration of the Directory, June 1993
SC21 N 7931	Working Document on the Internationalization of the Directory, June 1993
SC21 N 7932	Enhancement of Directory Operational Security, June 1993
SC21 N 7942	Directory Sch ma Migration, June 1993 (NWI Proposal)
SC21 N 7955	SC21/WG4 Standing Document 1: Issues for Extended Systems Management Architecture, July 1993
SC21 N 7957	Extended Systems Management Architecture, July 1993

SC21 N 7959	Expiry Behavior, second WD, July 1993
SC21 N 7962	Working Document for Command Sequencer for Systems Management, July 1993
SC21 N 7965	Definition of Systems Management Protocol Machine Managed Objects, September 1993
SC21 N 7970	Enhanced Functionality for Systems Management Communications, June 1993
SC21 N 7980	Liaison Statement to ITU-TS/SG15 on Change Over Function, August 1993
SC21 N 7983	Liaison Statement to SC21/WG8 and SC27 on Future Liaison Activity, SC21/WG4, August 1993
SC21 N 7991	Liaison Statement to JTC1/SC18, SC25, SC27, SC29, ISO/TC68, ISO/TC46, and JTC1/WG3 Concerning Activity on Quality of Service, SC21/WG1, August 1993
SC21 N 7992	Liaison Statement to ISO/TC184/SC5/WG2 Concerning Activity on Quality of Service, SC21/WG1, August 1993
SC21 N 7993	Quality of Service Framework, Second Working Draft, August 1993 (rapporteur meeting November 1993; PDTR expected July 1994)
SC21 N 7995	Working Draft on Formal Methods in Conformance Testing, September 1993 (collaborative meeting February 1994; CD expected July 1994)
SC21 N 8003	NP on Architecture for Multipeer Data Communications, June 1993
SC21 N 8004	Liaison Statement to ISO/TC184/SC5/WG2 on Question 65.1—User Requirements for OSI Systems Supporting Time Critical Communications, SC21/WG1, August 1993
SC21 N 8005	Liaison Statement to ITU-TS/SG7 (Q2/7, Q19/7, Q20/7) on Quality of Service, SC21/WG1, August 1993
SC21 N 8010	Open Systems Assessment Methodology, June 1993 (NWI Proposal; ballot ended November 1993) (CD expected 1995)
SC21 N 8011	Conformance Testing of OSI Protocols over OSI Services Provided by Non-OSI Protocols, July 1993 (NWI Proposal; ballot ended November 1993) (PDAMs to 9646-1 to -7 expected June 1995)
SC21 N 8013	Liaison Statement to JTC1/SWG-CA, JTC1/SGFS, EWOS, OIW, and AOW on Open Systems Assessment Methodology, August 1993
SC21 N 8016	Extensions to ISO 9646 on Testing of OSI Protocols over OSI Services Provided by Non-OSI Protocols, June 1993 (NWI Proposal; ballot ended November 1993)
SC21 N 8018	Liaison Statement to ITU-TS SG7 (Q19/7) on Q1/65.2—OSI Protocols Efficiency, August 1993
SC21 N 8019	Liaison Statement to ITU-TS/SG7 on Q1/67 - Generalization of ASO Concept, SC21/WG1, August 1993
SC21 N 8020	Liaison Statement to JTC1/SC27 on Open Systems Security, SC21/WG1, August 1993
SC21 N 8022	NP on Enhancements to LOTOS, June 1993
SC21 N 8023	Initial Draft on Enhancements to LOTOS, SC21/WG1, November 1993
SC21 N 8029	Liaison Statement to JTC1/SC6 on Quality of Service, SC21/WG1, August 1993
SC21 N 8030	Liaison Statement to EWOS, OIW, and AOW on Quality of Service, SC21/WG1, August 1993
SC21 N 8034	Liaison Statement to the Object Management Group, SC21/WG7, August 1993
SC21 N 8037	Issues for Management Domain Management Function, June 1993
SC21 N 8040	Relationship Management Function, Second Working Document, June 1993
SC21 N 8045 Rev	Report of the SC21 Study Group on APIs, Revised, June 1993.
SC21 N 8056	SC21 SWG-MF Meeting, June 1993, Yokohama, July 1993
SC21 N 8057	Recommendation to Progress Work on the Use of Standard Data Modelling Facilities in the Preparation of International Standards, SWG-MF, July 1993
SC21 N 8058	Final Recommendations of the SC21 Special Working Group on Modelling Facilities (SWG-MF), SWG-MF, July 1993
SC21 N 8059	Response to the SC21 Chairman from the SC21 Special Working Group on Modelling Facilities (SWG-MF), SWG-MF, July 1993
SC21 N 8060	Conceptual Schema Modeling Facility, June 1993 (NWI Proposal; ballot ended November 1993) (rapporteur meeting January 1994)
SC21 N 8061	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to ISO/IEC JTC1/SC18 Liaison Statement, SWG-MF, July 1993
SC21 N 8062	SC21 Special Working Group on Modelling Facilities (SWG-MF) Liaison Statement to ISO/IEC JTC1/SC14, SWG-MF, July 1993
SC21 N 8063	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to ISO/IEC JTC1/WG3 Open edi Liaison Report, SWG-MF, July 1993
SC21 N 8064	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to ISO/TC46/SC4 Liaison Statement, SWG-MF, July 1993
SC21 N 8065	SC21 Special Working Group on Modelling Facilities (SWG-MF) Response to JTC1/SC21/WG7 Liaison Statement, SWG-MF, July 1993
SC21 N 8081	Resolutions of the Ninth Plenary Meeting of ISO/IEC JTC1/SC 21, 29-30 June 1993, Yokohama, Japan, June 1993
SC21 N 8103 Rev.	Request from SC21 to JTC1 Concerning the "Fast Tracking" of the PCTE Document, June 1993
SC21 N 8109	Proposed New Question Q3/011, "Harmonization of Client/Server Capabilities," SC21/WG3, September 1993
SC21 N 8118	Report from the SC21 ISP Meeting, 23 June 1993, Yokohama, June 1993

SC21 N 8122	Management Guidelines, June 1993
SC21 N 8122	Update to Management Guidelines on Formal Descriptions, SC21, June 1993
SC21 N 8127	Liaison Information on Modelling Facility Interim Work, SC21 SWG-MF, June 1993
SC21 N 8128	Liaison Statement to the Internet Society, SC21, June 1993
SC21 N 8129	Statement of Benefits on Establishment of C-Liaison with X/Open, SC21, June 1993
SC21 N 8130	Statement of Benefits on Establishment of C-Liaison with the Object Management Group (OMG), SC21, June 1993
SC21 N 8131	Statement of Benefits on Establishment of C-Liaison with the Internet Society, SC21, June 1993
SC21 N 8151	Status of Work on the Subtransactions in OSI TP, SC21/WG8, July 1993
SC21 N 8152	Status of Work on the Separation of Data and Commit Flows in OSI TP, SC21/WG8, July 1993
SC21 N 8161	Working Draft on Enhancements to Metric Objects and Attributes, SC21/WG4, July 1993
SC21 N 8162	Working Draft for ICS Proforma for Metric Objects and Attributes, SC21/WG4, July 1993
SC21 N 8163	Working Draft for ICS Proforma for Summarization Function, SC21/WG4, July 1993
SC21 N 8173	Information Processing Systems - Open Systems Interconnection - Basic Presentation Service Definition, review text of the Edition 2 of ISO 8822, August 1993
SC21 N 8174	Information Processing Systems - Open Systems Interconnection - Basic Connection Oriented Presentation Protocol, Part 1: Protocol Specification, review text of the Edition 2 of ISO 8823-1, August 1993
SC21 N 8178	Working Document on Managed Objects for Upper Layers, August 1993
SC21 N 8192	Working Document on Topic 9.1 - ODP Trader, August 1993 (CD expected July 1994)
SC21 N 8193	Status of X.Series Recommendations, ITU-TS SG7, August 1993
SC21 N 8202	Working Draft on IRDS Services Interface Extensions, September 1993
SC21 N 8204	Working Draft on IRDS Framework Standard (Revision of ISO 10027:1990), September 1993
SC21 N 8205	SQL Multimedia and Hypermedia Application Packages (SQL/MM) Project Plan (Revised), SC21/WG3, September 1993
SC21 N 8211	Draft Answer to Question Q3/007, "Support for Distributed Database Systems," SC21/WG3, September 1993
SC21 N 8216	Working Draft of Conformance Test Suite for the TP Protocol, Part 1: Test Suite Structure and Test Purposes, September 1993 (CD expected July 1994)
SC21 N 8218	Working Draft for Information Technology - Open Distributed Processing - Basic Reference Model of ODP, Part 1: Overview and Guide to Use, September 1993
SC21 N 8249	Rules of Procedure and Working Methods of the ITU Telecommunications Standardization Sector and Study Group Responsibility and Mandates, ITU-TS, October 1993
SC21 N 8251	Proposed Approval of 27 Recommendations Agreed to by Study Group 7 at its Meeting on 2 July 1993, ITU-TS, October 1993
SC21 N 8256	Disposition of Comments Report and Final Work Item Definition for "Engagement Scheduling and Recording Application within the Distributed Office Applications Model (DOAM)," October 1993
SC21 N 8256	Liaison Statement Regarding FTAM Abstract Test Suites, EWOS/EG FT, October 1993
SC21 N 8258	Corrected Liaison Statement to SC21 Entitled, "Comments on the First Draft Report on the New Work Area on Programmatic Interfaces," SC18, October 1993
SC21 N 8260	Liaison to SC21 on the Character, Graphic Symbol and Glyph, SC18/WG8, October 1993
SC21 N 8261	Liaison Between SC24 and SC21, SC24, October 1993
SC21 N 8262	Liaison Statement to SC21 and SC6 on OSI Quality of Service, ITU-TS SG7, October 1993
SC21 N 8263	Liaison Statement to SC21 and SC6 on OSI Quality of Service Framework Specifications, ITU-TS SG7, October 1993
SC21 N 8264	Liaison Statement to SC21/WG1 Conformance Group on Collaborative Work, ITU-TS/SG7, October 1993
SC21 N 8265	Liaison Statement to SC21 on OSI Service Conventions, ITU-TS SG7, October 1993
SC21 N 8266	Liaison Statement to SC21 on OSI Reference Model, ITU-TS SG7, October 1993
SC21 N 8267	Liaison Statement to SC21 on OSI Multicast Architecture, ITU-TS SG7, October 1993
SC21 N 8268	Liaison Statement to SC21 WGs 1 and 8 on OSI Protocol Efficiency to ICG on Satellite Matters, SG8, SG11, SG13, ISO/IEC JTC1/SC21 (WGs 1 and 8), and ISO/JTC1/SG6, ITU-TS SG7, October 1993
SC21 N 8269	Liaison Statement to SC21 WG/8 on Security Activities, ITU-TS SG7, October 1993
SC21 N 8270	Liaison Statement to SC21 WG/8 on the ROSE Standard, ITU-TS SG7, October 1993
SC21 N 8280	Liaison Statement to SC21/WG4 on Requirements and Directions for the Use of Formal Description Techniques for the Specification of Managed Objects, ITU-TS SG7, October 1993
SC21 N 8281	Liaison Statement to SC21/WG4 Concerning the OSI Systems Management Implementor's Guide, ITU-TS SG7, October 1993
SC21 N 8282	Calling Notice and Draft Agenda for the Interim Meeting of the SC21/WG3 Rapporteur Group on Conceptual Schema Modelling Facilities, Aix en Provence, 17-21 January 1994, October 1993
SC21 N 8285	Position on the ODP Standards Process and Cooperation with de facto Standards Organizations, AFNOR, October 1993
SC21 N 8305	A Data Modelling Facility: JDMF/MODEL-1992, Japan, October 1993

SC21 N 8315	Question on Registration of Names of International Organizations for Directory, USA, October 1993
SC21 N 8316	Comments on Standardized Programmatic Interfaces, USA, October 1993
SC21 N 8318	Establishment of Formal Liaison Between JTC1/SC21 and JTC1/SC29, SC29, December 1993
SC21 N 8320	UK Position on Programmatic Interface Standardization, UK, November 1993
SC21 N 8321	Requirement for Partial Rollback, USA, November 1993
SC21 N 8322	Response to SC21 N 8067 on TP with RPC, USA, November 1993
SC21 N 8325	Authentication and Privilege Attribute Security Application with Related Key Distribution Functions, Part 1: Overview and Functional Model, ECMA/TC-TG9, November 1993
SC21 N 8326	Authentication and Privilege Attribute Security Application with Related Key Distribution Functions, Part 2: Security Information Objects, ECMA/TC-TG9, November 1993
SC21 N 8327	Authentication and Privilege Attribute Security Application with Related Key Distribution Functions, Part 3: Service Definitions, ECMA/TC-TG9, November 1993
SC21 N 8328	Liaison Statement to SC21/WG8 Regarding Authentication and Related Security Services for Distributed Applications, ECMA/TC-TG9, November 1993
SC21 N 8329	Liaison Contribution to SC21/WG8 Regarding Authentication and Related Security Services for Distributed Applications - Extended Schematic for First Draft, ECMA/TC-TG9, November 1993
SC21 N 8330	Version V2 of the APA-Application Standard, ECMA/TC-TG9, November 1993 (standard has three parts: Overview and Functional Model, Security Information Objects, and Service Definitions)
SC21 N 8355	Liaison Statement to SC21/WG1 and SC22/WG15 on Conformance Testing, December 1993
SC21 N 8356	Draft Technical Corrigenda to ISO 8571, FTAM, December 1993
SC21 N 8380	Guide to Open System Security, Working Draft Technical Report, December 1993
SC21 N 8382	Liaison Statement to SC21/WG4 on Management of Time Critical Communications, ISO/TC184/SC5/WG2, December 1993
SC21 N 8383	Liaison Statement to SC21/WG1 on Question 65.1—User Requirements for OSI Systems Supporting Time Critical Communications, ISO/TC184/SC5/WG2, December 1993
SC21 N 8384	Liaison Statement to SC21/WG1 on Multi-Peer Data Transmission, ISO/TC184/SC5/WG2, December 1993
SC21 N 8385	Final Draft Version of TCCA Technical Report (DTR 12178) Sent to the ISO Central Secretariat for Publication, ISO/TC184/SC5/WG2, December 1993
SC21 N 8397	Outline Contribution to Future Work as Proposed in SC21 N 8045 Rev 2, SC21 SWG-SPI Meeting 8-11 November 1993 in Torina, January 1994
SC21 N 8409	Information Technology - Open Systems Interconnection - ODP Trading Function, January 1994
SC21 N 8410	Methodology and Guidelines for the Development of Application Layer Protocols, January 1994

DOCUMENTS OF SC21 WORKING GROUPS

SC21/WG1 N 1140	UK Discussion Paper on Conformance Testing for OSI Security
SC21/WG1 N 1156	Clarification on Use of the PICS
SC21/WG1 N 1157	Contributions on LOTOS Enhancements
SC21/WG1 N 1253	Use of Quality of Services in ODP Trader, May 1993
SC21/WG3 N 1279	Report of Meeting CDIF/1175/PDES Information Coordination
SC21/WG3 N 1283	IRDS Services Interface Extensions - Design Document
SC21/WG3 N 1298	New Project Proposal: SQL ADT Packages
SC21/WG3 N 1345	Letter to Convenor, Government Telecommunications Agency/VPD, Ottawa Canada, EWOS, Expert Group on Database Enquiry
SC21/WG3 N 1349	Liaison Report June 1991-May 1992, JTC1/SC7 Software Engineering
SC21/WG3 N 1371	Discussion between JTC1 SC21/WG3 and ISO TC 184/SC5/WG4
SC21/WG3 N 1406	Agreed Scope of Work for the Revision of the IRDS Framework (IS 10027), Ottawa
SC21/WG3 N 1430	DBL Status Report
SC21/WG3 N 1557 Rev	Proposal for the Registration of Q3/010: ODP and Distributed Database Systems, June 1993
SC21/WG3 N 1581	Distributed Data and the Scope of Federated Database Systems, June 1993
SC21/WG3 N 1586	Views on the Relationship Between the ODP Trader and Data Management, June 1993
SC21/WG3 N 1613	ISO SQL Multimedia and Application Packages (SQL/MM), Part 2: Full-Text, Working Draft, September 1993
SC21/WG3 N 1614	ISO SQL Multimedia and Application Packages (SQL/MM), Part 3: Spatial, Working Draft, September 1993
SC21/WG3 N 1644	Technical Report on the Semantic Unification of Meta-Model, Volume 1, Semantic Unification of Static Models, US National Body, November 1993
SC21/WG3 N 1645	Knowledge Interchange Format (KIF), US National Body, Nnovember 1993
SC21 WG3 N 1646	Proposed Working Draft for Base Document for Conceptual Schema Modelling Facilities, October 1993
SC21/WG3 N 1647	ISO SQL Multimedia and Application Packages (SQL/MM), Part 1: Framework, Working Draft, October 1993

SC21/WG3 N 1653	RMDM, SQL92 and SQL3 Mapping Final Reports—Summary and Conclusions, Final V1.1, Inkron Inc., August 1993
SC21/WG3 N 1655	Liaison Statement to CSMF RG, December 1993
SC21/WG3 N 1660	Applicability of the ISO Reference Model of Data Management (ISO 10032:1993) to Client Server Computing, Dr. T. William Olle, October 1993
SC21/WG4 N 1438	UK Contribution to 21/63.2, Testability of Managed Objects
SC21/WG4 N 1451	Comments on SC21 N 6749: NP Time Services in an OS
SC21/WG4 N 1472	US Response to SC21 N 6679, Request for National Body Comments on the Progression of an Amendment to ISO/IEC 10164-11 on the Definition of Multiple Input Metric Objects
SC21/WG4 N 1527	Closing WG4 Plenary Report on Directory Meeting, Ottawa
SC21/WG4 N 1641	Issues for Extended Systems Management Architecture (WG4 SD 1), December 1992
SC21/WG4 N 1831	Second Working Draft on Expiry Behavior, December 1993
SC21/WG4 N 1832	Command Sequencer, Working Draft, December 1993
SC21/WG4 N 1853	Manager Role Conformance, Second Working Draft, December 1993
SC21/WG5 N 673	Minutes of the TP Group Meeting, Ottawa, 21-29 May 1992
SC21/WG6 N 1123	UK Position on Alignment of Upper and Lower Layer Security Protocols
SC21/WG6 N 1124	UK Comment on SC21 N 6130, Generic Transfer Syntax Providing Upper Layers Security
SC21/WG6 N 1125	UK Contribution on Lightweight Encoding Rules for ASN.1
SC21/WG6 N 1152	Proposals for Changes to SC21/WG6 Programme of Work
SC21/WG6 N 1155	Provision of Guidance on Application of XALS Concepts
SC21/WG6 N 1158	Strawman Generic Security ESO-OSI Abstract Interface
SC21/WG6 N 1159	Proposal for a New Work Item on a Class of Mappings from a Single ASN.1 Type to an FTAM Document Type
SC21/WG6 N 1171	ASN.1 Information Objects, Constraints, Parameterization - Tutorial and Worked Examples, D.A. Steedman, Editor
SC21/WG7 N 743	Working Document on Topic 9.1 - ODP Trader, November 1992
SC21/WG7 N 783	An Integrated Approach to Trader Contexts, August 1993
SC21/WG7 N 811	Relations of Formal Descriptions of Different ODP Viewpoint Models, August 1993
SC21/WG7 N 821	Discussion Note on RM-ODP Part 4, August 1993
SC21/WG7 N 823	Joint Action Plan SC21/WG7 and WG7-ITU-TS/Q16/7 (ITU-TS Format), August 1993
SC21/WG7 N 836	Liaison Contributions for SC21/WG7, SC21/WG3, August 1993
SC21/WG7 N 852	Outline of Information Specification for ODP Trader, Australia, October 1993
SC21/WG7 N 862	An ODP Architectural Semantics in Z, UK, October 1993
SC21/WG7 N 863	An ODP Architectural Semantics in LOTOS, UK, October 1993
SC21/WG8 N 173	Authentication and Related Security Services, Part 2: Generic Abstract Services for Security (GASS), Strawman, November 1993

II. ITU-TS RECOMMENDATIONS[3]

A. F-Series, Telematic Services
B. I-Series, ISDN Services
C. Q-Series, ISDN Internetworking
D. T-Series, Telematic Services
E. V-Series
F. X-Series, Public Data Networks
G. Z-Series

A. ITU-TS F-SERIES, TELEMATIC SERVICES

F.11	Continued Availability of Traditional Services
F.30 Rev 1	Use of Various Sequences of Combinations for Special Purposes
F.40	International Public Telemessage Service
F.41	Interworking Between the Telemessage Service and the International Public Telegram Service
F.59	General Characteristics of the International Telex Service
F.63 Rev 1	Additional Facilities in the International Telex Service
F.69 Rev 1	Plan for Telex Destination Codes
F.72 Rev 1	International Telex Store and Forward - General Principles and Operational Aspects
F.73	Operational Principles For Communication Between Terminals on Telex Networks and Data Terminal Equipment on Packet Switched Public Data Networks (PSPDNs)
F.80	Basic Requirements for Interworking Relations Between the International Telex Service and Other Services
F.82	Operational Provisions to Permit Interworking Between the International Telex Service and the Intex Service
F.86	Interworking Between the International Telex Service and DE Videotex Service
F.87	Operational Principles for the Transfer of Messages from Terminals of the International Telex Service to Group 3 Facsimile Terminals Connected to the Public Switched Telephone Network
F.104	International Leased Circuit Services - Customer Circuit Designations
F.111	Principles of Service for Mobile Systems
F.140 Rev 1	Point-to-Multipoint Telecommunication Service Via Satellite
F.150	Service and Operational Provision for the Intex Service
F.160 Rev 1	General Operational Provisions for the International Public Facsimile Services
F.180 Rev 1	General Operational Provisions for the International Public Facsimile Service Between Subscribers' Stations (Telefax)
F.182 Rev 1	Operational Provisions for the International Public Facsimile Service Between Subscriber Stations with Group 3 Facsimile Machines (Telefax 3)
F.184 Rev 1	Operational Provisions for the International Public Facsimile Service Between Subscriber Stations with Group 4 Facsimile Machines (Telefax 4)
F.200	Teletex Service
F.200/C	Teletex Service, Annex C: Mixed Mode of Operation
F.201 Rev 1	Internetworking Between the Teletex Service and the Telex Service
F.220 Rev 1	Service requirements Unique to the Processable Mode Number One (PM1)
F.300 Rev 1	Videotext Service
F.400	Message Handling System and Service Overview
F.401	Naming and Addressing for Public Message Handling Services
F.410	The Public Messaging Transfer Service
F.415	Intercommunication with Public Physical Delivery Services
F.420	The Public Interpersonal Messaging (IMP) Service
F.421	Intercommunication Between the IPM Service and the Telex Service

3 ITU-TS Recommendations are final versions of 1988 documents (Blue Book) unless otherwise indicated. Updated from *Catalogue of New CCITT Recommendations*, CCITT circular 118, 12 November 1991. The ITU-TS information was updated from *Results of the First World Telecommunication Standardization Conference*, SC21 N 7751, 20 April 1993 and from *Report on ITU-TS Study Group 7 Program of Work and Collaboration with SC21*, SC21 N 7887, June 1993.

F.422	Intercommunication Between the IPM Service and the Teletex Service
F.435	Message Handling Systems: Electronic Data Interchange (EDI) Messaging System, 1991
F.500	International Public Directory Services
F.551	Service Recommendation for Telematic File Transfer Within Telefax 3, Telefax 4, Teletex and Message Handling Services
F.581	Guidelines for Programming Communication Interfaces Definition (Service Recommendation)
F.600 Rev 1	Service and Operational Principles for Public Data Transmission Services
F.710	General Principles for Audiographic Conference Services
F.850	Principles of Universal Personal Telecommunication
F.901	Usability Evaluation of Telecommunication Services

B. ITU-TS G-SERIES AND I- SERIES, ISDN SERVICES

G.703	Metallic Media
G.707 to G.709	SDH Rates and Format
G.774	Management Information Model
G.781 to G.784	Equipment Functions
G.803	Network Architecture
G.831	Management capabilities
G.957	Optical Interfaces
G.958	Line Systems

I.100 Series General Concepts, Terminology, and General Methods

I.110	Preamble and General Structure of the I-Series Recommendations
I.111	Relationship with Other Recommendations Relevant to ISDNs
I.112 Rev 1	Vocabulary of Terms for ISDNs
I.113	Vocabulary of Terms for Broadband Aspects of ISDNs
I.114	Vocabulary of Terms for Universal Personal Telecommunication
I.120	Integrated Service Digital Networks (ISDNs)
I.121	Broadband Aspects of ISDNs
I.122 Rev 1	Framework for Providing Additional Packet Mode Bearer Services
I.130	Method for the Characterization of Telecommunications Services Supported by an ISDN and Network Capabilities of an ISDN
I.140 Rev 1	Attribute Technique for the Characterization of Telecommunication Services Supported by an ISDN and Network Capabilities of an ISDN
I.141	ISDN Network Charging Capabilities Attributes
I.144	Number Identification Supplementary Services
I.150 Rev 1	B-ISDN Asynchronous Transfer Mode Functional Characteristics

I.200 Series Service Aspects

I.200	Guidance to the I.200 Series of Recommendations (service aspects)
I.210 Rev 1♦[4]	Principles of Telecommunications Services Supported by an ISDN and the Means to Describe Them
I.211 Rev 1♦	B-ISDN Service Aspects
I.212♦	Teleservices Supported by an ISDN
I.220	Common Dynamic Description of Basic Telecommunication Services
I.221 Rev 1	Common Specific Characteristics of Services
I.223.1	ISDN Frame Mode Bearer Services (FMBS) - ISDN Frame Relaying Bearer Services
I.223.2	ISDN Frame Mode Bearer Services (FMBS) - ISDN Frame Switching Bearer Service
I.230	Definition of Bearer Service Categories
I.231♦	Circuit-Mode Bearer Service Categories
I.231.9♦	Circuit Mode 64 kbit/s 8 kHz Structured Multi-Use Bearer Service Category
I.232♦	Packet Mode Bearer Service Categories
I.240♦	Definition of Teleservices
I.241♦	Teleservices Supported by an ISDN
I.241.7♦	Telephony 7 kHz
I.250♦	Definition of Supplementary Services
I.251	Number Identification Supplementary Services
I.252	Call Offering Supplementary Services
I.253	Call Completion Supplementary Services

4 The symbol ♦ is used throughout this section to identify those recommendations included in the September 1993 *NOSIP Strategy* [Ref. NATO 1993].

I.253.1	Call Waiting (CW) Supplementary Service
I.254	Multiparty Supplementary Services
I.255	Community of Interest Supplementary Services
I.255.3	Multilevel Precedence and Preemption Service (MLPP) - Description Preference Service
I.255.4	Priority of Service
I.256	Charging Supplementary Services
I.256.2a	Advice of Charge: Charging Information at Call Set-Up Time
I.256.2b	Advice of Charge: Charging Information During Call
I.256.2c	Advice of Charge: Charging Information at End of the Call
I.257	Additional Information Transfer Supplementary Services
I.300 Series	**Network Aspects**
I.310 Rev 1	ISDN - Network Functional Principles
I.311 Rev 1	B-ISDN General Network Aspects
I.320•	ISDN Protocol Reference Model
I.321	B-ISDN Protocol Reference Model and Its Application
I.324	ISDN Network Architecture
I.325 Rev 1	Reference Configurations for ISDN Connection Types
I.326	Reference Configurations for Relative Network Resource Requirements
I.327 Rev 1	B-ISDN Functional Architecture
I.330	ISDN Numbering and Addressing Principles
I.331	Numbering Plan for the ISDN Era
I.332	Numbering Principles for Interworking Between ISDNs and Dedicated Networks with Different Numbering Plans
I.333 Rev 1	Terminal Selection in ISDN
I.334	Principles Relating ISDN Numbers/Subaddresses to the OSI Reference Model Network Layer Addresses
I.335	ISDN Routing Principles
I.340	ISDN Connection Types
I.350 Rev 1	General Aspects of Quality of Service and Network Performance in Digital Networks, Including ISDNs
I.351 Rev 1	Recommendations in Other Services Including Network Performance Objectives that Apply at Reference Point T of an ISDN
I.352 Rev 1	Network Performance Objectives for Connection Processing Delays in an ISDN
I.353	Reference Events for Defining ISDN Performance Parameters
I.354	Network Performance Objectives for Packet-Mode Communication in an ISDN
I.355	ISDN 64 Kbit/s Connection Type Availability Performance
I.361 Rev 1	B-ISDN ATM Layer Specification
I.362 Rev 1	B-ISDN ATM Adaptation Layer (AAL) Functional Description
I.363 Rev 1	B-ISDN ATM Adaptation Layer (AAL) Specification
I.364	Support of Broad Band Connectionless Data Service on B-ISDN
I.370	Congestion Management for the ISDN Frame Relaying Bearer Service
I.371	Traffic Control and Congestion Control in B-ISDN
I.372	Frame Relaying Bearer Service Network-to-Network Interface Requirements
I.373	Network Capabilities to Support Universal Personal Telecommunication
I.374	Framework Recommendation on Network Capabilities to Support Multimedia Services
I.400 Series	**User network interface aspects**
I.410	General Aspects and Principles Relating to Recommendations on ISDN User-Network Interfaces
I.411 Rev 1	ISDN User-Network Interfaces—Reference Configurations
I.412	ISDN User-Network Interfaces—Interface Structures and Access Capabilities
I.413 Rev 1	B-ISDN User Network Interface
I.414	Overview of Recommendations on Layer 1 for ISDN and B-ISDN Customer Accesses
I.420	Basic User-Network Interface (ISDN)
I.421	Primary Rate User-Network Interface (ISDN)
I.430 Rev 1	Basic User-Network Interface—Layer 1 Specification (ISDN)
I.431 Rev 1•	Primary Rate User-Network Interface—Layer 1 Specification (ISDN)
I.432 Rev 1•	B-ISDN Network Interface—Physical Layer Specification
I.440•	ISDN User-Network Interface —Data Link Layer General Aspects (Q.920)
I.441•	ISDN User-Network Interface—Data Link Layer Specification (Q.921)
I.450•	ISDN User-Network Interface—Layer 3 General Aspects (Q.930)
I.451•	ISDN User-Network Interface—Layer 3 Specification for Basic Call Control (Q.931)
I.452•	ISDN User-Network Interface—Layer 3 Specification - Generic Procedures for the Control of the ISDN Supplementary Services (Q.932)
I.453(?)•	ISDN User-Network Interface - Protocol for Management - General Aspects (Q.940)

I.460•	Multiplexing, Rate Adaptation and Support of Existing Interfaces (ISDN)
I.461•	Support of X.21, X.21 bis, and X.20 bis Based DTEs by an ISDN (X.30)
I.462•	Support of Packet Mode Terminal Equipment by an ISDN (X.31)
I.463•	Support of DTEs with V-Series Type Interfaces by an ISDN
I.464•	Multiplexing, Rate Adaptation, and Support of Existing Interfaces for Restricted 64 kbit/s Transfer Capability
I.465	Support by an ISDN of DTEs with V-Series Type Interfaces with Provisions for Statistical Multiplexing
I.470	Relationship of Terminal Functions to ISDN
I.500 Series Internetwork Interfaces	
I.500 Rev 1	General Structure of the ISDN Interworking Recommendations
I.501	Frame Mode Bearer Services (FMBS) Interworking
I.510 Rev 1	Definitions and General Principles for ISDN Interworking
I.511	ISDN to ISDN Layer 1 Internetwork Interface
I.515 Rev 1	Parameter Exchange for ISDN Interworking
I.520 Rev 1	General Arrangement for Network Interworking Between ISDNs
I.525	Interworking between ISDN and Networks which Operate at Bit Rates less than 64 kbit/s
I.530 Rev 1	Network Interworking Between an ISDN and a Public Switched Telephone Network (PSTN)
I.540	General Arrangement for Network Interworking Between Circuit Switched Public Data Networks (CSPDNs) and ISDNs for the Provision of Data Transmission Services
I.550	General Arrangement for Network Interworking Between Packet Switched Public Data Networks (PSPDNs) and ISDNs for the Provision of Data Transmission Services
I.560	Requirements to be Met in Providing the Telex Service Within the ISDN
I.570	Public/private ISDN Interworking
I.580	General Arrangements for Interworking Between B-ISDN and 64 kbit/s Based ISDN
I.600 Series Maintenance Principles	
I.601	General Maintenance Principles of ISDN Subscriber Access and Subscriber Installation
I.602	Application of Maintenance Principles to ISDN Subscriber Installation
I.603	Application of Maintenance Principles to ISDN Basic Accesses
I.604	Application of Maintenance Principles to ISDN Primary Rate Accesses
I.605	Application of Maintenance Principles to Static Multiplexed ISDN Basic Accesses
I.610 Rev 1	OAM Principles of the B-ISDN access

C. ITU-TS Q-SERIES, ISDN INTERNETWORKING

Q.700•	Signaling System No. 7 (SS7) Overview
Q.701-Q.710•	Signaling System No. 7 (SS7) Message Transfer Part
Q.711-Q.716•	Signaling System No. 7 (SS7) Signalling Connection Control Part (SCCP)
Q.720-Q.729•	Signaling System No. 7 (SS7) Telephone User Part (TUP)
Q.730-Q.739•	Signaling System No. 7 (SS7) ISDN Supplementary Services
Q.760-Q.769•	Signaling System No. 7 (SS7) Description of the ISDN User Part (ISUP)
Q.770-Q.779•	Signaling System No. 7 (SS7) Transaction Capabilities (TC)

D. ITU-TS T-SERIES, TELEMATIC SERVICES

T.0	Classification of Facsimile Apparatus for Document Transmission over the Public Networks
T.4 Rev 3	Standardization of Group 3 Facsimile Apparatus for Document Transmission
T.5	General Aspects of Group 4 Facsimile Apparatus
T.6	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus
T.22	Standardized Test Charts for Document Facsimile Transmissions
T.30 Rev 3	Procedures for Document Facsimile Transmission in the General Switched Telephone Network
T.35	Procedure for the Allocation of Defined Codes for Non-Standard Facilities
T.50	International Alphabet No. 5
T.51	Coded Character Sets for Telematic Services
T.52	Non-Latin Coded Character Sets for Telematic Services
T.60 Rev 1	Terminal Equipment for Use in the Teletex Service
T.61 Rev 1	Character Repertoire and Coded Character Sets for the International Teletex Service
T.62 Rev 1	Control Procedures for Teletex and Group 4 Facsimile Services
T.62 bis Rev 1	Control Procedures for Teletex and Group 4 Facsimile Services Based on Recommendations X.215/X.225
T.63 Rev 1	Provision for Verification of Teletex Terminal Compliance
T.64 Rev 1	Conformance testing procedures for the teletex Recommendations

T.70 Rev 1♦	Network-Independent Basic Transport Service for the Telematic Services
T.71	LAPB Extended for Half-Duplex Physical Level Facility
T.72	Terminal Capabilities for Mixed Mode of Operation
T.73	Document Interchange Protocol for the Telematic Services
T.82	Coded Representation of Picture and Audio Information-Progressive Bi-level Image Compression
T.90	Teletex Requirements for Internetworking with the Telex Service
T.91	Teletex Requirements for Real-Time Internetworking with the Telex Service in a Packet-Switching Network Environment
T.101 Rev 1	International Interworking for Videotex Services
T.102	Protocols for Syntax-Based Videotex Using ISDN Circuit Mode
T.103	Protocols for Syntax-Based Videotex Using ISDN Packet Mode
T.104	Packet Mode Access for Syntax-Based Videotex Via PSTN
T.105	Syntax-Based Videotex Application Layer Protocol
T.106	Framework for Videotex Terminal Protocols
T.122	Multipoint Communications Service
T.123	Protocol Stacks For Audiographic And Audiovisual Teleconference Applications
T.330	Telematic Access to Interpersonal Messaging System
T.400	Introduction to Document Architecture, Transfer and Manipulation
T.410/S	First extension (January 1991) to the T.410 Series (1988) of Recommendations contained in the Blue Book, Fascicle VII.6
T.411	Open Document Architecture (ODA) and Interchange Format - Introduction and General Principles (see ISO 8613-1)
T.411/F	Annex F to T.411 Recommendation
T.412	Open Document Architecture (ODA) and Interchange Format - Document Structures (see ISO 8613-2)
T.414	Open Document Architecture (ODA) and Interchange Format - Document Profile (see ISO 8613-4)
T.415	Open Document Architecture (ODA) and Interchange Format - Open Document Interchange Format (ODIF) (see ISO 8613-5)
T.416	Open Document Architecture (ODA) and Interchange Format - Character Content Architectures (see ISO 8613-6)
T.417	Open Document Architecture (ODA) and Interchange Format - Raster Graphics Content Architectures (see ISO 8613-7)
T.418	Open Document Architecture (ODA) and Interchange Format - Geometric Graphics Content Architectures (see ISO 8613-8)
T.419	Document Transfer and Manipulation (DTAM) - Composite Graphics Content Architectures
T.431	Document Transfer and Manipulation (DTAM) - Services and Protocols, Introduction and General Principles
T.432	Document Transfer and Manipulation (DTAM) - Services and Protocols, Service Definition
T.433	Document Transfer and Manipulation (DTAM) - Services and Protocols, Protocol Specification
T.441	Document Transfer and Manipulation (DTAM) - Operational Structure
T.501 Rev 1	Document Application Profile MM for the Interchange of Formatted Mixed Mode Documents (Mixed Mode)
T.502 Rev 1	Document Application Profile PM11 for the Interchange of Processable Form Documents (Teletex Processable Mode)
T.503	A Document Application Profile for the Interchange of Group 4 Facsimile Documents
T.504 Rev 1	Document Application Profile for Videotex Interworking
T.505	Document application profile PM-26 for the interchange of mixed content documents in processable and format forms
T.510 Rev 1	Overview of sub-series T.510 Recommendations
T.521	Communication Application Profile BT0 for Document Bulk Transfer Based on the Session Service (According to Rules Defined in T.62 bis)
T.522	Communication Application Profile BT1 for Document Bulk Transfer
T.523 Rev 1	Communication Application Profile DM-1 for Videotex Interworking
T.541 Rev 1	Operational Application Profile for Videotex Interworking
T.561	Terminal Characteristics for Mixed Mode of Operation MM
T.562	Terminal Characteristics for Teletex Processing Mode PM1
T.563 Rev 1	Terminal Characteristics for Group 4 Facsimile Apparatus
T.564 Rev 1	Gateway Characteristics for Videotex Interworking

E. ITU-TS V-SERIES

V.1♦	Equivalence Between Binary Notation Symbols and Sign, Condition of a Two-Condition Code
V.4♦	General Structure of Signals of International Alphabet No. 5 Code for Data Transmission over PTN

V.5♦	Standardization of Data Signalling Rates for Synchronous Data Transmission in the General Switched TN
V.6♦	Standardization of Data Signalling Rates for Synchronous Data Transmission on Leased Telephone-Type Circuits
V.7♦	Definition of Terms Concerning Data Communication over Telephone Network
V.10/X.26 Rev 1♦	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communication
V.11/X.27 Rev 1♦	Electrical Characteristics for Balanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communications
V.13	Simulated Carrier Control
V.14	Transmission of Start-Stop Characters over Synchronous Bearer Channels
V.17	A 2-Wire Modem for Facsimile Applications With Rates up to 14,400 bit/s
V.20	Telex and Gentex Signalling on Radio Channels (Synchronous 7-Unit Systems Affording Error Correction by Automatic Repetition)
V.24 Rev 1♦	List of Definitions for Interchange Circuits Between DTE and DCE
V.25	Automatic Answering Equipment and/or Parallel Automatic Calling Equipment on the General Switched Telephone Network Including Procedures for Disabling of Echo Control Devices for Both Manually and Automatically Established Calls
V.25 bis	Automatic Calling and/or Answering Equipment on the General Switched Telephone Network (GSTN) Using the 100-Series Interchange Circuits
V.28 Rev 1♦	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits
V.31	Electrical Characteristics for Single-Current Interchange Circuits Controlled by Contact Closure
V.31 bis	Electrical Characteristics for Single-Current Interchange Circuits Using Opto Couplers
V.32 Rev 1	A Family of 2-Wire, Duplex Modems Operating at Data Signaling Rates of up to 9,600 bit/s for Use on the General Switched Telephone Network and on Leased Telephone-Type Circuits
V.32 bis	A Duplex Model Operating at Data Signalling Rates of up to 14,400 bit/s for Use on the General Switched Telephone Network and on Leased Point-to-Point 2-Wire Telephone-Type Circuits
V.35♦	Data Transmission at 48 kbit/s Using 60-108 kHz Group Band Circuits
V.36♦	Modems for Synchronous Data Transmission Using 60-108 kHz Group Band Circuits
V.37♦	Synchronous Data Transmission at a Data Signalling Rate Higher than 72 kbit/s Using 60-108 kHz Group Band Circuits
V.38	A 48/56/64 kbit/s Data Circuit Terminating Equipment Standardized for Use On Digital Point-to-Point Leased Circuits
V.42 Rev 1	Error-Correcting Procedures for DCEs Using Asynchronous-to-Synchronous Conversion
V.42 bis	Data Compression Procedures For Data Circuit Terminating Equipment (DCE) Using Error Correcting Procedures
V.54	Loop Test Devices for Modems

F. ITU-TS X-SERIES[5]

PUBLIC DATA NETWORKS: Services and Facilities

X.1 Rev 1♦	International User Classes of Service in and Categories of Access to Public Data Networks and Integrated Services Digital Networks (ISDNs), 1993
X.2 Rev 1	International Data Transmission Services and Optional User Facilities in Public Data Networks and ISDNs, 1993
X.3 Rev 1	Packet Assembly/Disassembly Facility (PAD) in a Public Data Network (PDN), 1993
X.4	General Structure of Signals of International Alphabet No. 5 Code for Data Transmission over Public Data Networks, 1988
X.5	Facsimile Packet Assembly/Disassembly Facility (FPAD) in a Public Data Network, 1992
X.6	Multicast Service Definition, 1993
X.7	Technical Characteristics of Data Transmission Services, 1993
X.10♦	Categories of Access for Data Terminal Equipment (DTE) to Public Data Transmission Services, 1993
X.asp	Multi-Aspect PAD Protocol Definitions-1, Draft, 1993 (approval target November 1994)
X.asp+	Multi-Aspect PAD Protocol Definitions-2, Draft, 1993 (approval target 1996)
X.atc	Address Translation Capability in Public Data Networks, Draft, 1993 (approval target November 1994)
X.map	Multi-Aspect PAD Framework, Draft, 1993 (approval target February 1994)

5 Updated from [SC21 N 8193 1993] (as of July 1993).

PUBLIC DATA NETWORKS: Interfaces

X.20 Rev 1	Interface Between DTE and DCE for Start-Stop Transmission Services on Public Data Networks, 1988
X.20 bis	Use on Public Data Networks of DTE which is Designed for Interfacing to Asynchronous Duplex V-Series Modems, 1988
X.21•	Interface Between DTE and DCE for Synchronous Operation on Public Data Networks, 1992
X.21 bis•	Use on Public Data Networks of DTE which is Designed for Interfacing to Synchronous V-Series Modems, 1988
X.22	Multiplex DTE/DCE Interface for User Classes 3-6, 1988
X.24•	List of Definitions for Interchange Circuits Between DTE and DCE on Public Data Networks, 1988
X.25 Rev 1•	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit, 1988 (Revised Edition, 1993)
X.26/V.10•	Electrical Characteristics for Unbalanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communications, 1993
X.27/V.11•	Electrical Characteristics for Balanced Double-Current Interchange Circuits for General Use with Integrated Circuit Equipment in the Field of Data Communications, 1993
X.28 Rev 1	DTE/DCE Interface for a Start/Stop Mode DTE Accessing the PAD in a PDN Situated in the Same Country, 1993
X.29 Rev 1	Procedures for the Exchange of Control Information and User Data Between a PAD Facility and a Packet Mode DTE or Another PAD, 1993
X.30/I.461 Rev 1	Support of X.21, X.21 bis, and X.20 bis Based Data Terminal Equipments (DTEs) by an ISDN, 1993
X.31/I.462 Rev 1•	Support of Packet Mode Terminal Equipment by an ISDN, 1993
X.32 Rev 1•	Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Accessing a Packet Switched PDN Through a Public Switched Telephone Network or a Circuit Switched PDN, 1993
X.35	Interface Between a PSPDN and a Private PSDN which is Based on X.25 Procedures and Enhancements to Define a Gateway Function that is provided in the PSPDN, Draft (ITU-TS balloting ended November 1993)
X.38	G3 Facsimile Equipment/DCE Interface for G3 Facsimile Equipment Accessing the Facsimile Packet Assembly/Disassembly Facility (FPAD) in a Public Data Network Situated in the Same Country, 1992
X.39	Procedures for the Exchange of Control Information and User Data Between a Facsimile Packet Assembly/Disassembly (FPAD) Facility and a Packet Mode DTE or Another FPAD, 1992
X.3x	Access to Packet Switched Data Transmission Services Provided by PSPDN or ISDN via Frame Relaying PDNs or ISDN Providing Frame Mode Bearer Service, Draft, 1993 (approval target November 1994)
X.fru	Interface Between DTE and DCE for Public Data Network Prroving Frame Relay Data Transmission Service, Draft, 1993 (approval target November 1994)
X.isp	Inter-Service Protocol for a Multicast Service, Draft, 1993 (approval target June 1995)
X.mcp	Procedures for the Provision of a Basic Multicast Service for DCEs Operating Using Recommendation X.25, Draft, 1993 (approval target November 1994)
X.mcp+	Procedures for the Provision of an Enhanced Multicast Service for DCEs Operating Using Recommendation X.25 and Requiring Additional Protocol, Draft, 1993 (approval target 1996)
X. mpc	Encapsulation in X.25 Packets of Various Protocols Including Frame Relay, Draft, 1993 (approval target November 1994)

PUBLIC DATA NETWORKS: Transmission, Signalling, and Switching

X.50	Fundamental Parameters of a Multiplexing Scheme for the International Interface Between Synchronous Data Networks, 1988
X.50bis	Fundamental Parameters of a 48-kbit/s User Data Signalling Rate Transmission Scheme for the International Interface Between Synchronous Data Networks, 1988
X.51	Fundamental Parameters of a Multiplexing Scheme for the International Interface Between Synchronous Data Networks Using 10-bit Envelope Structure, 1988
X.51bis	Fundamental Parameters of a 48-kbit/s User Data Signalling Rate Transmission Scheme for the International Interface Between Synchronous Data Networks Using 10-bit Envelope Structure, 1988
X.52	Method of Encoding Anisochronous Signals into a Synchronous User Bearer, 1988
X.53 Rev 1	Numbering of Channels on International Multiplex links at 64 kbit/s, 1993
X.54	Allocation of Channels on International Multiplex Links at 64 kbit/s, 1988
X.55	Interface Between Synchronous Data Networks Using a 6+2 Envelope Structure and Single Channel Per Carrier (SCPC) Satellite Channels, 1988
X.56	Interface Between Synchronous Data Networks Using an 8+2 Envelope Structure and Single Channel Per Carrier (SCPC) Satellite Channels, 1988
X.57	Method of Transmitting a Single Lower Speed Data Channel on a 64 kbit/s Data Stream, 1988
X.58	Fundamental Parameters of a Multiplexing Scheme for the International Interface Between Synchronous Non-Switched Data Networks Using No Envelope Structure, 1988
X.60	Common Channel Signalling for Circuit Switched Data Applications, 1988
X.61/Q.741	Signalling System No. 7 - Data User Part, 1988

X.70	Terminal and Transit Control Signalling System for Start-Stop Services on International Circuits Between Anisochronous Data Networks, 1988
X.71	Decentralized Terminal and Transit Control Signalling System on International Circuits Between Synchronous Data Networks, 1988
X.75 Rev 1•	Packet-Switched Signalling System Between Public Networks Providing Data Transmission Services, 1988 (Revised Edition, 1993)
X.7x	Signalling System Between Public Networks Providing Frame Relaying Data Transmissional Services, Draft, 1993 (approval date November 1994)
X.80	Interworking of Interexchange Signalling Systems for Circuit Switched Data Services, 1988
X.81	Interworking Between an ISDN Circuit-Switched and a Circuit-Switched Public Data Network (CSPDN), 1988
X.82	Detailed Arrangements for Interworking Between CSPDNs and PSPDNs Based on Recommedation T.70, 1988
PUBLIC DATA NETWORKS: Network Aspects	
X.92	Hypothetical Reference Connections for Public Synchronous Data Networks, 1988
X.96 Rev 1	Call Progress Signals in Public Data Networks, 1993
X.110	International Routing Principles and Routing Plan for Public Data Networks, 1988
X.121	International Numbering Plan for Public Data Networks, 1992
X.122/E.166	Numbering Plan Interworking for the E.164 and X.121 Numbering Plans, 1992
X.130	Call Processing Delays in Public Data Networks when Providing International Synchronous Circuit-Switched Data Services, 1988
X.131	Call Blocking in Public Data Networks when Providing International Synchronous Circuit-Switched Data Services, 1988
X.134	Portion Boundaries and Packet Layer Reference Events: Basis for Defining Packet-Switched Performance Parameters, 1992
X.135	Speed of Service (Delay and Throughput) Performance Values for Public Data Networks when Providing International Packet-Switched Services, 1992
X.136	Accuracy and Dependability Performance Values for Public Data Networks when Providing International Packet-Switched Services, 1992
X.137	Availability Performance Values for Public Data Networks when Providing International Packet-Switched Services, 1992
X.138	Measurement of Performance Values for Public Data Networks when Providing International Packet-Switched Services, 1992
X.139	Echo, Drop, Generator and Test DTE's for Measurement of Performance Values for Public Data Networks when Providing International Packet-Switched Services, 1992
X.140	General Quality of Service Parameter for Communication Via Public Data Networks, 1992
X.141	General Principles for the Detection and Correction of Errors in Public Data Networks, 1988 (with corrections)
X.frq	User Information Transfer Parameters and Specifications for Data Networks Providing International Frame Relay PVC Service, Draft, 1993 (approval date November 1994)
PUBLIC DATA NETWORKS: Maintenance	
X.150	Principles of Maintenance Testing for Public Data Networks Using DTE and DCE Test Loops, 1988
X.160	Architecture for Customer Network Management Services for Public Data Networks, Draft, 1993 (approval date February 1994)
X.161	Definition of Customer Network Management Services for Public Data Networks, Draft, 1993 (approval date November 1994)
X.162	Definition of Management Informaton for the Customer Network Management Services for Public Data Networks, Draft, 1993 (approval date November 1994)
PUBLIC DATA NETWORKS: Administrative Arrangements	
X.180	Administrative Arrangements for International Closed User Groups (CUGs), 1988
X.181	Administrative Arrangements for the Provision of International Permanent Virtual Circuits (PVCs), 1988
OPEN SYSTEMS INTERCONNECTION: Model and Notation	
X.200	Information Technology - Open Systems Ineroonnection - Reference Model: Basic Reference Model (ISO/IEC 7498), 1988 (approval date for Revision 1 November 1994)
X.207	Information Technology - Open Systems Ineroonnection - Application Layer Structure (ISO 9545) (ITU-TS ballot ended November 1993)
X.208	Specification of Abstract Syntax Notation One (ASN.1) (ISO 8824), 1988 (see X.680)
X.209	Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) (ISO 8825), 1988 (see X.690)
X.210:1988	OSI Layer Service Definition Conventions (ISO 8509), 1988
X.210:1993	Conventions for Definitions of OSI Services (ISO 10731), Draft, 1993 (revision submitted for ITU-TS ballot that ended November 1993)
X.211	Physical Service Definition of OSI for CCITT Applications (ISO 10022), 1988
X.212	Data Link Service Definition of OSI for CCITT Applications (ISO 8886), 1988

X.213	Network Service Definition of OSI for CCITT Applications (ISO 8348), 1992 (approval date for common text with ISO/IEC November 1994)
X.214	Transport Service Definition of OSI for CCITT Applications (ISO 8072), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.215	Session Service Definition for OSI for CCITT Applications (ISO 8826), 1988 (approval date for common text with ISO/IEC February 1994)
X.216	Presentation Service Definition for OSI for CCITT Applications (ISO 8822), 1988 (approval date for common text with ISO/IEC February 1994)
X.217	Service Definition for the Association Control Service Element (ISO 8649), 1992 (approval date for common text with ISO/IEC November 1994)
X.218 Rev 1	Reliable Transfer: Model and Service Definition (ISO 9066-1), 1993
X.219	Remote Operations: Model, Notation and Service Definition (ISO 9072-1), 1988 (see X.880 and X.881)
OPEN SYSTEMS INTERCONNECTION: Connection-mode Protocol Specifications	
X.220 Rev 1	Use of X.200-Series Protocols in CCITT Applications, 1993
X.222	Use of X.25 LAPB to Provide the OSI Connection-mode Data Link Service (Appendix III of X.212), 1988 (approval date for common text with ISO/IEC November 1994)
X.223	Use of X.25 to Provide the OSI Connection-mode Network Service for CCITT Applications (ISO 8878], 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.224	Protocol for Providing the OSI Connection-mode Transport Service (ISO 8073), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.225	Session Protocol Specification for OSI for CCITT Applications (ISO 8327), 1988 (approval date for common text with ISO/IEC February 1994)
X.226	Presentation Protocol Specification for OSI for CCITT Application (ISO 8823), 1988 (approval date for common text with ISO/IEC February 1994)
X.227	Protocol Specification for the Association Control Service Element (ISO 8650), 1992 (approval date for common text with ISO/IEC November 1994)
X.228	Reliable Transfer: Protocol Specification (ISO 9066-2), 1988
X.229	Remote Operations: Protocol Specification (ISO 9072-2), 1988 (see X.882)
OPEN SYSTEMS INTERCONNECTION: Connectionless-mode Protocol Specifications	
X.233	Information Technology - Open Systems Interconnection - Protocol for Providing Connectionless-Mode Network Service (ISO 8473-1), Draft, 1993 (submitted for ITU-TS ballot that ended November 1993)
X.234	Information Technology - Open Systems Interconnection - Protocol for Providing the OSI Connectionless-Mode Transport Service (ISO 8602), Draft, 1993 (approval date February 1994)
X.235	Information Technology - Open Systems Interconnection - Connectionless-Mode Session Protocol: Protocol Specification (ISO 9548), Draft, 1993 (approval date November 1994)
X.236	Information Technology - Open Systems Interconnection - Connectionless-Mode Presentation Protocol: Protocol Specification (ISO 9576), Draft, 1993 (approval date February 1994)
X.237	Information Technology - Open Systems Interconnection - Connectionless-Mode Protocol Specification for the Association Control Service Element (ISO 10035), 1992
OPEN SYSTEMS INTERCONNECTION: Miscellaneous	
X.244	Procedure for the Exchange of Protocol Identification During Virtual Call Establishment on Packet Switched Public Data Networks, 1988
X.245	Information Technology - Open Systems Interconnection - Connection-Mode Session Protocol: PICS Proforma (ISO 8327-2), Draft, 1993 (approval date November 1994)
X.246	Information Technology - Open Systems Interconnection - Connection-Mode Presentation Protocol: PICS Proforma (ISO 8823-2), Draft, 1993 (approval date February 1994)
X.247	Information Technology - Open Systems Interconnection - Connection-Mode Protocol Specification for the Association Control Service Element: PICS Proforma (ISO 8650-2), Draft, 1993 (approval date February 1994)
X.248	Reliable Transfer Service Element - PICS Proforma, 1992
X.249	Remote Operations Service Element - PICS Proforma, 1992
X.255	Information Technology - Open Systems Interconnection - Connectionless-Mode Session Protocol: PICS Proforma (ISO 9548-2), Draft, 1993 (approval date February 1994)
X.256	Information Technology - Open Systems Interconnection - Connectionless-Mode Presentation Protocol: PICS Proforma (ISO 9576-2), Draft, 1993 (approval date February 1994)
X.257	Information Technology - Open Systems Interconnection - Connectionless-Mode ACSE Protocol: PICS Proforma (ISO 10035-2), Draft, 1993 (approval date February 1994)
OPEN SYSTEMS INTERCONNECTION: Protocol Identification	
X.263	Network Protocol Identification Mechanism (TR 9577), Draft, 1993 (approval date November 1994)
X.264	Transport Protocol Identification Mechanism (ISO 11570), Draft, 1993 (submitted for ITU-TS ballot that ended November 1993)

OPEN SYSTEMS INTERCONNECTION: Security Protocols

X.273	Information Technology - Open Systems Interconnection - Network Layer Security Protocol (ISO 11577), Draft, 1993 (approval target February 1994)
X.274	Information Technology - Open Systems Interconnection - Transport Layer Security Protocol (ISO 10736), Draft, 1993 (approval target February 1994)

OPEN SYSTEMS INTERCONNECTION: Layer Managed Objects

X.281	Elements of Management Information Related to the OSI Physical Layer (ISO 13642), Draft, 1993 (approval target June 1995)
X.282	Elements of Management Information Related to the OSI Data Link Layer (ISO 10742), Draft, 1993 (approval target February 1994)
X.283	Elements of Management Information Related to the OSI Network Layer (ISO 10733) (submitted for ITU-TS ballot that ended November 1993)
X.284	Elements of Management Information Related to the OSI Transport Layer (ISO 10737), Draft, 1993 (approval target February 1994)
X.290	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: General Concepts (DIS 9646-1), 1992 (approval target for revision and common text with ISO/IEC November 1994)
X.291	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: Abstract Test Suite Specifications (ISO 9646-2), 1992 (approval target for revision and common text with ISO/IEC November 1994)
X.292	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: TTCN (ISO 9646-3), 1992 (approval target for revision and common text with ISO/IEC November 1994)
X.293	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: Test Realization (ISO 9646-4), 1992 (approval target for revision and common text with ISO/IEC November 1994)
X.294	OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications: Requirements on Test Labsoratories and Clients for Conformance Assessment Process (ISO 9646-5), 1992 (approval target for revision and common text with ISO/IEC November 1994)
X.295	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework - Protocol Profile Test Specification (ISO 9646-6), Draft, 1993 (approval target November 1994)
X.296	Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework - Implementation Conformance Statements (ISO 9646-7), Draft, 1993 (approval target November 1994)

INTERWORKING BETWEEN NETWORKS: General

X.300	General Principles and Arrangements for Interworking Between Public Data Networks, and Between Public Data Networks and Other Public Networks, 1988
X.301 Rev 1	Description of the General Arrangement for Call Control Within a Subnetwork and Between Subnetworks for the Provision of Data Transmission Services, 1993
X.302	Description of the General Arrangement for Internal Network Utilities Within a Subnetwork and Immediate Utilities Between Subnetworks for the Provision of Data Transmission Services, 1988
X.305	Functionalities of Subnetworks Relating to the Support of the OSI Connection-Mode Network Service, 1988
X.320	General Arrangements for Interworking Between ISDNs for the Provision of Data Transmission Services, 1988 (approval target of revision June 1995)
X.321/I.540	General Arrangements for Interworking Between Circuit Switched Public Data Networks (CSPDNs) and ISDNs for the Provision of Data Transmission Services, 1988 (approval target of revision June 1995)
X.322	General Arrangements for Interworking Between Packet Switched Public Data Networks (PSPDNs) and CSPDNs for the Provision of Data Transmission Services, 1988
X.323	General Arrangements for Interworking Between PSPDNs, 1988
X.324	General Arrangements for Interworking Between PSPDNs and Public Mobile Systems for the Provision of Data Transmission Services, 1988
X.325	General Arrangements tor Interworking Between PSPDNs and ISDNs for the Provision of Data Transmission Services, 1988 (approval target of revision June 1995)
X.326	General Arrangements for Interworking Between PSPDNs and Common Channel Signalling Network (CCSN), 1988
X.327	General Arrangements for Interworking Between PSPDNs and Private Data Networks for the Provision of Data Transmission Services, 1988 (ITU-TS balloting of revision ended November 1993)
X.340 Rev 1	General Arrangements for Interworking Between PSPDNs and the International Telex Network, 1993
X.3fi	General Arrangements for Interworking Between Frame Relaying Public Data Networks and ISDNs, Draft, 1993 (approval target November 1994)

X.350	General Interworking Requirements to be Met for Data Transmission in International Public Mobile Satellite Systems, 1988
X.351	Special Requirements to be Met for Packet Assembly/Disassembly Facilities (PADs) Located at or in Association with Coast Earth Stations in the Public Mobile Satellite Service, 1988
X.352	Interworking Between Packet Switched Public Data Networks and Public Maritime Mobile Satellite Data Transmission Systems, 1988
X.353	Routing Principles for Interconnecting Public Maritime Mobile Satellite Data Transmission Systems with Public Data Networks, 1988
INTERWORKING BETWEEN NETWORKS: Management	
X.370	Arrangements for the Transfer of Internetwork Management Information, 1988
MESSAGE HANDLING SYSTEMS	
X.400/F.400 Rev 1	Message Handling Systems (MHSs): Message Handling System and Service Overview (ISO 10021-1), 1993 (approval target for common text with ISO/IEC November 1994)
X.401	MHSs - Basic Service Elements and Optional User Facilities, 1984 (discontinued)
X.402	MHSs - Overall Architecture (ISO 10021-2), 1992 (approval target for common text with ISO/IEC November 1994)
X.403	MHSs - Conformance Testing, 1988
X.407	MHSs - Abstract Service Definition Conventions (ISO 10021-3), 1988 (approval target for revision and common text with ISO/IEC November 1994)
X.408	MHSs - Encoded Information-Type Conversion Rules, 1988
X.409	MHSs - Presentation Transfer Syntax and Notation, 1984 [replaced by X.208 (ISO 8824 with DAD 1) and X.208 (ISO 8825 with DAD 1)] (discontinued)
X.410	MHSs - Remote Operations and Reliable Transfer Server, 1984 [replaced by X.218 (ISO 9066-1), X.219 (ISO 9072-1), X.228 (ISO 9066-2), and X.229 (ISO 9072-2)] (discontinued)
X.411	MHSs - Message Transfer System: Abstract Service Definition and Procedures (ISO 10021-4), 1992 (approval target for common text with ISO/IEC November 1994)
X.413	MHSs - Message Store: Abstract Service Definition (ISO 10021-5), 1992 (approval target for common text with ISO/IEC November 1994)
X.419	MHSs - Protocol Specifications (ISO 10021-6), 1992 (approval target for common text with ISO/IEC November 1994)
X.420	MHSs - Interpersonal Messaging Sysem (ISO 10021-7), 1992 (approval target for common text with ISO/IEC November 1994)
X.421	COMFAX Use of MHS, Draft, 1993 (approval target February 1994)
X.435	Message Handling Systems: Electronic Data Interchange (EDI) Messaging System, 1991 (fast-track balloting in ISO/IEC)
X.440	Message Handling Systems: Voice Messaging System, 1992
X.480	Message Handling Systems and Directory Services Conformance Testing, 1992
X.481	MHSs - P2 Protocol: PICS Proforma, 1992
X.482	MHSs - P1 Protocol: PICS Proforma, 1992
X.483	MHSs - P3 Protocol: PICS Proforma, 1992
X.484	MHSs - P7 Protocol: PICS Proforma, 1992
X.485	MHSs - Voice Messaging System PICS Proforma, 1992
X.4acc	Information Technology - Communication - Message Handling System (MHS): Computer Conferencing, Draft, 1993
X.4ae	MHS Management: Access Unit Entity, Draft, 1993 (approval target 1995-1996)
X.4agc	Information Technology - Communication - Message Handling System (MHS): Group Communication, Draft, 1993
X.4cm	MHS Management: Configuration Management Function, Draft, 1993 (approval target 1995-1996)
X.ep	Information Technology - Message Handling Systems - PICS Proforma for EDIMG, Draft, 1993 (approval target November 1994)
X.4fm	MHS Management: Fault Management Function, Draft, 1993 (approval target 1995-1996)
X.4gm/X.inf	MHS Management: Information and Functional Overview, Draft, 1993 (approval target 1995-1996)
X.4ma	MHS Management: Accounting Management, Draft, 1993 (approval target November 1994)
X.4me	MHS Management: Message Store Entity, Draft, 1993 (approval target 1995-1996)
X.4mma	MHS Management: Model and Architecgture, Draft, 1993 (approval target November 1994)
X.4mo	MHS Management: MTA Management, Draft, 1993 (approval target 1995)
X.4pm	MHS Management: Performance Management Function, Draft, 1993 (approval target 1995-1996)
X.4sm	MHS Management: Security Management, Draft, 1993 (approval target June 1995)
X.4ue	MHS Management: User Agent Entity, Draft, 1993 (approval target 1995-1996)
DIRECTORY	
X.500	Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models, and Services (ISO 9594-1), 1988 (revision submitted for ITU-TS ballot that ended November 1993)

X.501	Information Technology - Open Systems Interconnection - The Directory: The Models (ISO 9594-2), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.509	Information Technology - Open Systems Interconnection - The Directory: Authentication Framework (ISO 9594-8), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.510	Overview of Sub-series X.510 Recommendations
X.511	Information Technology - Open Systems Interconnection - The Directory: Abstract Service Definition (ISO 9594-3), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.518	Information Technology - Open Systems Interconnection - The Directory: Procedures for Distributed Operation (ISO 9594-4), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.519	Information Technology - Open Systems Interconnection - The Directory: Protocol Specification (ISO 9594-5), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.520	Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types (ISO 9594-6), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.521	Information Technology - Open Systems Interconnection - The Directory: Selected Object Classes (ISO 9594-7), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.525	Information Technology - Open Systems Interconnection - The Directory: Replication (ISO 9594-9), 1988 (revision submitted for ITU-TS ballot that ended November 1993)
X.581	Directory Access Protocol - PICS Proforma, 1992 (ISO 9594-10 being fast-tracked)
X.582	Directory System Protocol - PICS Proforma, 1992 (ISO 9594-10 being fast-tracked)
OSI NETWORKING AND SYSTEM ASPECTS: Networking	
X.610	Provision and Support of the OSI Connection-Mode Network Service, 1992
X.612	Information Technology - Provision of the OSI Connection-Mode Network Service by Packet Mode Terminal Equipment Connected to an ISDN, 1992
X.613	Information Technology - Use of X.25 Packet Layer Protocol in Conjunction with X.21/X.21 bis to Provide the OSI Connection-Mode Network Service, 1992
X.614	Information Technology - Use of X.25 Packet Layer Protocol in Conjunction with X.21/X.21 bis to Provide the OSI Connection-Mode Network Service over the Telephone Network, 1992
X.615	Information Technology - Provision of the OSI Connection-Mode Network Service over Frame Relay, 1992
X.620	Information Technology - Provision and Support of the OSI Connection-Mode Network Service over Frame Relay, 1992
X.622	Information Technology - Use of X.25 Packet Layer Protocol in Conjunction with X.21/X.21 bis to Provide the OSI Connection-Mode Network Service over the Telephone Network, 1992
X.623	Information Technology - Use of X.25 Packet Layer Protocol in Conjunction with X.21/X.21 bis to Provide the OSI Connection-Mode Network Service over the Telephone Network, 1992
OSI NETWORKING AND SYSTEM ASPECTS: Naming, Addressing, and Registration	
X.650	Information Technology - Open Systems Innterconnection - Basic Reference Model: Naming and Addressing (ISO 7498-3), 1992
X.660	Information Technology - Open Systems Innterconnection - Procedures for the Operation of OSI Registration Authorities: General Procedures (ISO 9834-1), 1992
X.662	Information Technology - Open Systems Innterconnection - Procedures for the Operation of OSI Registration Authorities: Registration of Object Identifier Component Values for Joint ISO-CCITT Use (ISO 9834-3), Draft, 1993 (target approval November 1994)
X.665	Information Technology - Open Systems Innterconnection - Procedures for the Operation of OSI Registration Authorities: Application Processes and Applicaion Entitite (ISO 9834-6), 1992
OSI NETWORKING AND SYSTEM ASPECTS: ASN.1	
X.680	Information Technology - Open Systems Innterconnection - ASN.1: Specification of Basic Notation, Basic ASN.1 (ISO 8824-1), Draft, 1993 (approval target February 1994) (see X.208)
X.681	Information Technology - Open Systems Innterconnection - ASN.1: Information Object Specification (ISO 8824-2), Draft, 1993 (approval target February 1994)
X.682	Information Technology - Open Systems Innterconnection - ASN.1: Constraint Specification (ISO 8824-3), Draft, 1993 (approval target February 1994)
X.683	Information Technology - Open Systems Innterconnection - ASN.1: Parameterization of ASN.1 Specifications (ISO 8824-4), Draft, 1993 (approval target February 1994)
X.690	Information Technology - Open Systems Innterconnection - Specification of ASN.1 Encoding Rules: Basic Encoding Rules (ISO 8825-1), Draft, 1993 (approval target February 1994) (see X.209)
X.691	Information Technology - Open Systems Innterconnection - Specification of ASN.1 Encoding Rules: Packet Encoding Rules (ISO 8825-1), Draft, 1993 (approval target June 1995)
X.692	Information Technology - Open Systems Innterconnection - Specification of ASN.1 Encoding Rules: Distinguished and Canonical Encoding Rules (ISO 8825-3), Draft, 1993 (approval target February 1994)

OSI MANAGEMENT

X.700	Management Framework for Open Systems Interconnection (OSI) for CCITT Applications (ISO 7498-4), 1992
X.701	Information Technology - Open Systems Innterconnection - Systems Management Overview (ISO 10040), 1992
X.702	Information Technology - Open Systems Innterconnection - Application Context for Systems Management for Transaction Processing (ISO 11587), Draft, 1993 (target approval June 1995)
X.710	Common Management Information Service Definition for CCITT Applications (ISO 9595), 1991
X.711	Common Management Information Protocol Specification for CCITT Applications (ISO 9596-1), 1991
X.712	Information Technology - Open Systems Innterconnection - Common Management Information Protocol: PICS Proforma (ISO 9596-2), 1992
X.720	Information Technology - Open Systems Innterconnection - Structure of Management Information: Management Information Model (ISO 10165-1), 1992
X.721	Information Technology - Open Systems Innterconnection - Structure of Management Information: Definition of Management Information (ISO 10165-2), 1992 (approval target for revision June 1995)
X.722	Information Technology - Open Systems Innterconnection - Structure of Management Information: Guidelines for the Definition of Managed Objects (ISO 10165-4), 1992
X.723	Information Technology - Open Systems Interconnection - Structure of Management Information - Generic Management Information (ISO 10165-5) (ITU-TS balloting ended November 1993)
X.724	Information Technology - Open Systems Interconnection - Structure of Management Information - Requirements and Guidelines for Implementation of Conformance Statement Proformas Associated with Management Information (ISO 10165-6) (ITU-TS balloting ended November 1993)
X.725	Information Technology - Open Systems Interconnection - Structure of Management Information - General Relationship Model (ISO 10165-7), Draft, 1993 (approval target June 1995)
X.730	Information Technology - Open Systems Interconnection - Systems Management: Object Management Function (ISO 10164-1), 1992 (approval target for revision November 1994)
X.731	Information Technology - Open Systems Interconnection - Systems Management: State Management Function ISO 10164-2), 1992 (approval target for revision November 1994)
X.732	Information Technology - Open Systems Interconnection - Systems Management: Attributes for Representing Relationships (ISO 10164-3), 1992 (approval target for revision November 1994)
X.733	Information Technology - Open Systems Interconnection - Systems Management: Alarm Reporting Function (ISO 10164-4), 1992 (approval target for revision November 1994)
X.734	Information Technology - Open Systems Interconnection - Systems Management: Event Report Management Function (ISO 10164-5), 1992 (approval target for revision November 1994)
X.735	Information Technology - Open Systems Interconnection - Systems Management: Log Control Function (ISO 10164-6), 1992 (approval target for revision November 1994)
X.736	Information Technology - Open Systems Interconnection - Systems Management: Security Alarm Report Function (ISO 10164-7), 1992 (approval target for revision November 1994)
X.737	Information Technology - Open Systems Interconnection - Systems Management: Confidence and Diagnosic Test Categories (ISO 10164-14), Draft, 1993 (approval target February 1994)
X.738	Information Technology - Open Systems Interconnection - Systems Management: Summarization Function (ISO 10164-13) (ITU-TS balloting ended November 1993)
X.739	Information Technology - Open Systems Interconnection - Systems Management: Metric Objects and Attributes (ISO 10164-11) (ITU-TS balloting ended November 1993)
X.740	Information Technology - Open Systems Interconnection - Systems Management: Security Audit Trail Function (ISO 10164-8), 1992
X.741	Information Technology - Open Systems Interconnection - Systems Management: Objects and Attributes for Access Control (ISO 10164-9), Draft, 1993 (approval target February 1994)
X.742	Information Technology - Open Systems Interconnection - Systems Management: Usage Metering Function (ISO 10164-10), Draft, 1993 (approval target February 1994)
X.743	Information Technology - Open Systems Interconnection - Systems Management: Time Management Function (ISO 10164-tm), Draft, 1993 (approval target 1998)
X.744	Information Technology - Open Systems Interconnection - Systems Management: Software Management Function (ISO 10164-sw), Draft, 1993 (approval target 1997)
X.745	Information Technology - Open Systems Interconnection - Systems Management: Test Management Function (ISO 10164-12) (ITU-TS balloting ended November 1993)
X.746	Information Technology - Open Systems Interconnection - Systems Management: Scheduling Function (ISO 10164-15), Draft, 1993 (approval target February 1994)
X.747	Information Technology - Open Systems Interconnection - Systems Management: General Relationship Function (ISO 10164-rm), Draft, 1993 (approval target 1997)
X.748	Information Technology - Open Systems Interconnection - Systems Management: Response Time Monitoring Function (ISO 10164-rtm), Draft, 1993 (approval target 1998)

X.749	Information Technology - Open Systems Interconnection - Systems Management: Management Domain Management Function (ISO 10164-md), Draft, 1993 (approval target 1997)
X.750	Information Technology - Open Systems Interconnection - Systems Management: Management Knowledge Management Function (ISO 10164-16), Draft, 1993 (approval target November 1994)
X.751	Information Technology - Open Systems Interconnection - Systems Management: Change Over Function (ISO 10164-co), Draft, 1993 (approval target 1997)
X.752	Information Technology - Open Systems Interconnection - Systems Management: Enhanced Event Control Function (ISO 10164-ev), Draft, 1993 (approval target 1997)
SECURITY	
X.800	Security Architecture for Open Systems Interconnection for CCITT Applications (ISO 7498-2), 1991
X.802	Information Technology - Open Systems Interconnection - Lower Layers Security Model (TR 13594), Draft, 1993 (approval target November 1994)
X.810	Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Security Authentication Frameworks Overview (ISO 18181-1), Draft, 1993 (approval target November 1994)
X.811	Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Authentication Framework (ISO 18181-2), Draft, 1993 (approval target February 1994)
X.812	Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Access Control Framework (ISO 18181-3), Draft, 1993 (approval target November 1994)
X.813	Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Non-Repudiation Framework (ISO 18181-4), Draft, 1993 (approval target November 1994)
X.814	Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Confidentiality Framework (ISO 18181-5), Draft, 1993 (approval target November 1994)
X.815	Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Integrity Framework (ISO 18181-6), Draft, 1993 (approval target November 1994)
X.816	Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems: Security Audit Framework (ISO 18181-7), Draft, 1993 (approval target November 1994)
X.830	Information Technology - Open Systems Interconnection - Generic Upper Layers Security - Security Eexchange Service Element: Overview, Model and notation (ISO 11586-1), Draft, 1993 (approval target November 1994)
X.831	Information Technology - Open Systems Interconnection - Generic Upper Layers Security: Security Eexchange Service Element (SESE) Service Definition (ISO 11586-2), Draft, 1993 (approval target November 1994)
X.832	Information Technology - Open Systems Interconnection - Generic Upper Layers Security: Security Eexchange Service Element (SESE) Protocol Specification (ISO 11586-3), Draft, 1993 (approval target November 1994)
X.833	Information Technology - Open Systems Interconnection - Generic Upper Layers Security: Protecting Transfe Syntax Specification (ISO 11586-4), Draft, 1993 (approval target November 1994)
X.834	Information Technology - Open Systems Interconnection - Generic Upper Layers Security: Security Eexchange Service Element (SESE) PICS Proforma (ISO 11586-5), Draft, 1993 (approval target November 1994)
X.835	Information Technology - Open Systems Interconnection - Generic Upper Layers Security: Security Eexchange Service Element (SESE) Protecting Transfer Syntax PICS Proforma (ISO 11586-6), Draft, 1993 (approval target November 1994).
COMMITMENT, CONCURRENCY AND RECOVERY	
X.851	Information Technology - Open Systems Interconnection - Service Definition of CCR Service Element, Edition 2 (ISO 9804) (submitted for ITU-TS ballot that ended November 1993)
X.852	Information Technology - Open Systems Interconnection - CCR Service Element: Protocol Specification (ISO 9805-1) (submitted for ITU-TS ballot that ended November 1993)
X.853	Information Technology - Open Systems Interconnection - CCR Service Element: PICS Proforma, Edition 2 (ISO 9805-2), Draft, 1993 (approval target February 1994)
TRANSACTION PROCESSING	
X.860	Distributed Transaction Perocessing: Model (ISO 10026-1), 1992
X.861	Distributed Transaction Perocessing: Service (ISO 10026-2), 1992
X.862	Distributed Transaction Perocessing: Protocol Specification (ISO 10026-3) (submitted for ITU-TS ballot that ended November 1993)
X.863	Information Technology - Open Systems Interconnection - Distributed Transaction Perocessing: PICS Proforma (ISO 10026-4), Draft, 1993 (approval target February 1994)
REMOTE OPERATIONS	
X.880	Information Technology - Remote Operations (RO), Part 1: Model, 1993 (CD 13712-1), Draft, 1993 (approval target February 1994)
X.881	Information Technology - Remote Operations (RO), Part 2: Service, 1993 (CD 13712-2), Draft, 1993 (approval target February 1994)

X.882	Information Technology - Remote Operations (RO), Part 3: Protocol, 1993 (CD 13712-3), Draft, 1993 (approval target February 1994)
X.883	Information Technology - Remote Operations (RO), Part 4: PICS Proforma, 1993 (CD 13712-4), Draft, 1993 (approval target February 1994)
OPEN DISTRIBUTED PROCESSING	
X.901	Information Technology - Basic Reference Model for Open Distributed Processing: Overview and Guide to Use (ISO 10746-1), Draft, 1993 (approval target 1996)
X.902	Information Technology - Basic Reference Model for Open Distributed Processing: Descriptive Model (ISO 10746-2), Draft, 1993 (approval target June 1995)
X.903	Information Technology - Basic Reference Model for Open Distributed Processing: Prescriptive Model (ISO 10746-3), Draft, 1993 (approval target June 1995)
X.904	Information Technology - Basic Reference Model for Open Distributed Processing: Architectural Semantics (ISO 10746-4), Draft, 1993 (approval target 1996)
X.tr	Information Technology - Basic Reference Model for Open Distributed Processing: Use of Formal Description Technique for ODP, Draft, 1993 (approval target 1996)
X.trader	Information Technology - Basic Reference Model for Open Distributed Processing: ODP Trader, Draft, 1993 (approval target 1996)

G. ITU-TS Z-SERIES

Z.100 Rev 1	Specification and Description Language (SDL)
Z.110	Criteria for the Use and Applicability of Formal Description Techniques
Z.120	Messages Sequence Charts
Z.200 Rev 1	High Level Language (CHILL) [DIS 9496.2]
Z.301	Introduction to the Man-Machine Language (MML)
Z.302	The Meta-Language for Describing MML Syntax and Dialogue Procedures
Z.311	Introduction to Syntax and Dialogue Procedures (MML)
Z.312	Basic Format Layout (MML)
Z.314	The Character Set and Basic Elements (MML)
Z.315	Input (Command) Language Syntax Specification (MML)
Z.316	Output Language Syntax Specification (MML)
Z.317	Man-Machine Dialogue Procedures (MML)
Z.321	Introduction to the Extended MML for Visual Display Terminals
Z.322	Capabilities of Visual Display Terminals (VDTs)
Z.323	Man-Machine Interaction
Z.331	Introduction to the Specification of the Man-Machine Interface
Z.332	Methodology for the Specification of the Man-Machine Interface - General Working Procedures
Z.333	Methodology for the Specification of the Man-Machine Interface - Tools and Methods
Z.341	Glossary of Terms (MML)
Z.351	Data-oriented Human-Machine Interface Specification Techniques, Part 1: Introduction
Z.352	Data-oriented Human-Machine Interface Specification Techniques, Part 2: Scope, Approach and Reference Model
Z.400	Structure and Format of Quality Manuals for Telecommunication Software

(This page intentionally left blank)

APPENDIX F

ORGANIZATIONS FOR STANDARDIZATION

ORGANIZATIONS FOR STANDARDIZATION[1]

1. INTRODUCTION

This appendix provides an overview of NATO organizations and other bodies with responsibility for standardization in the fields of communications and information systems. Eventually, this appendix is intended to be expanded to show specific responsibilities of each of the standards bodies. Where appropriate, the charts show the class of STANAGs or other standards maintained by each organization. The emphasis in this appendix is on technical standards for data communications.

2. NATO STANDARDS BODIES

Figure F-1 (foldout) identifies the NATO bodies with responsibility for standardization in communications and information systems. The chart only shows the NATO bodies for which staff support is provided by the NATO Headquarters' staffs, with the exception of those associated with the NATO Communications and Information Systems Organization (NACISO). Operational requirements are the responsibility of the Military Committee, primarily through the Military Agency for Standardization (MAS). Procedural standards are the responsibility of the Allied Data Systems Interoperability Agency (ADSIA), which reports to the Military Committee through the NACISO. Technical standards are the responsibility of the Tri-Service Group on Communications and Electronics (TSGCE).

Many groups in NATO produce standards. A substantial part of the work takes place within the structure of the Conference of National Armaments Directors (CNAD), and is mainly concerned with material standardization. The Military Agency for Standardization (MAS) is exclusively concerned with standardization, primarily in the operational field. Specific topics are also dealt with by other groups under the Military Committee.

In 1983 the North Atlantic Council decided to establish a NATO Standardization Group (NSG) composed of national representatives from both the operational and materiel-oriented sides of defence departments, and representatives from the Major NATO Commands (MNCs), the International Staff (IS), the International Military Staff (IMS) and the MAS. The purpose of the Group is to provide a multi-national forum for the harmonization of national views and the pursuit of NATO standardization activities. The Group is responsible to the Council for obtaining national and staff inputs with a view to the preparation of a composite NATO Standardization Programme (NSP) to be submitted to the NATO Standardization Tasking Authorities, after approval by the Council, for subsequent implementation.[2]

2.1 NATO Technical Standards Bodies

TSGCE has created a number of subgroups (SGs) and Project Groups (PGs) to develop and maintain technical standards for NATO. The subgroups and selected working groups (WGs) are:[3]

- SG4 on Navigation and Position Finding
- SG5 on Identification; seeks to enhance the interoperability of current identification equipment and to ensure the standardization, where necessary, to the NATO Identification System (NIS)
  - WG4 on Question and Answer (Q&A) System Interoperability; dedicated to Mark X/Mark XII issues, but will consider issues affecting the optimum implementation of the NATO Q&A
  - WG5 on Transition to the NIS Q&A
  - WG6 on Data Processing
- SG9 on Data Distribution; focuses on the development of data communications protocols, specifically for the NATO OSI Reference Model
  - WG4 on Data Links
  - WG5 on Profiles
  - WG6 on Pan-Layer Issues
  - Ad Hoc Working Group (AHWG) on Security

---

1 Appendix revised February 1994 based on informal contirbutions; *Guide to IT Standards Makers and Their Standards* [Ref. TA 1991]; and P1003.0 [Ref. IEEE 1992].

2 *The North Atlantic Treaty Organization--Facts and Figures* [NATO 1989].

3 *NATO Bodies in the Fields of Communications and Information Systems* [NACISC 1988] and *Directory--U.S. Participants in the International C3 Fora* [USMCEB 1989].

  - AHWG on Integrated Services Digital Network (ISDN)
  - PG3 on Multinational Information Distribution System (MIDS)
- SG11 on Tactical Communications
  - WG1 on Tactical Area Communications; seeks cooperation among the NATO nations in the development and procurement of tactical area communications for national forces
  - WG8 on Satellite Communications (SATCOM) Systems; seeks SATCOM interoperability between NATO and national military SATCOM systems
  - PG6 on Tactical Communications Systems for the Land Combat Zone--Post 2000; seeks, through a coordinated program, tactical communications systems designed to common standards
- SG12 on Information Systems
  - WG2 on Data Processing and Management
  - AHWG on Army Tactical Command and Control Information System (ATCCIS) (convened in conjunction with the meetings of the Technical Subgroup of the ATCCIS Permanent Working Group).

There are still two Project Groups reporting directly to the TSGCE:

- PG7 on Battlefield Information and Exploitation Systems (BICES)
- Special Working Group (SWG) on Ada Programming Support Environment (APSE), formed by 10 nations in 1987 to provide an environment in which tools can work together effectively to support information systems projects for the total development life cycle.

Liaison among these bodies (e.g., PG6 and SG9) is normally at the Secretary level. Plans are coordinated in annual meetings of the Secretaries and Action Officers of the Allied Tactical Communications Agency (ATCA), the Allied Naval Communications Agency (ANCA), the Allied Communications and Computer Security Agency (ACCSA), and the communications subordinate groups of TSGCE.[4]

To a limited degree, technical standards are also being addressed in the NATO Industrial Advisory Group (NIAG), specifically in SG6 on Compatibility of Naval Data Handling Equipment. NIAG SG6 is making recommendations on standards to be used in shipboard combat systems for data distribution, such as the Network Independent Interface (NIIF).

Table F-1 and Figure F-2 highlight the relationships among the NATO standards bodies whose responsibilities will be discussed in a chart that follows. To clarify the relationships among the organizations and to emphasize those bodies concerned with technical standards, some of the NATO bodies have been left out and most of the names have been replaced with acronyms. Table F-1 provides the definitions of the acronyms for Figure F-2.

2.2 NATO OSI Standards Bodies

TSGCE SG9 has responsibility for the NATO OSI Reference Model and developing OSI STANAGs. SG9 also maintains the *NTIS Transition Strategy* [Purton 1987] that contains intercept recommendations.

TSGCE SG9 meets biannually, usually in March and October. Beginning in 1990, SG9 will meet approximately 6 to 8 weeks after the fall meetings of WG1 and WG2, to allow time for the nations to coordinate positions on issues developed by the working groups. Thus, the next meeting of SG9 is December 1990, while WG1 and WG2 will meet in October 1990. AHWGs meet approximately quarterly.

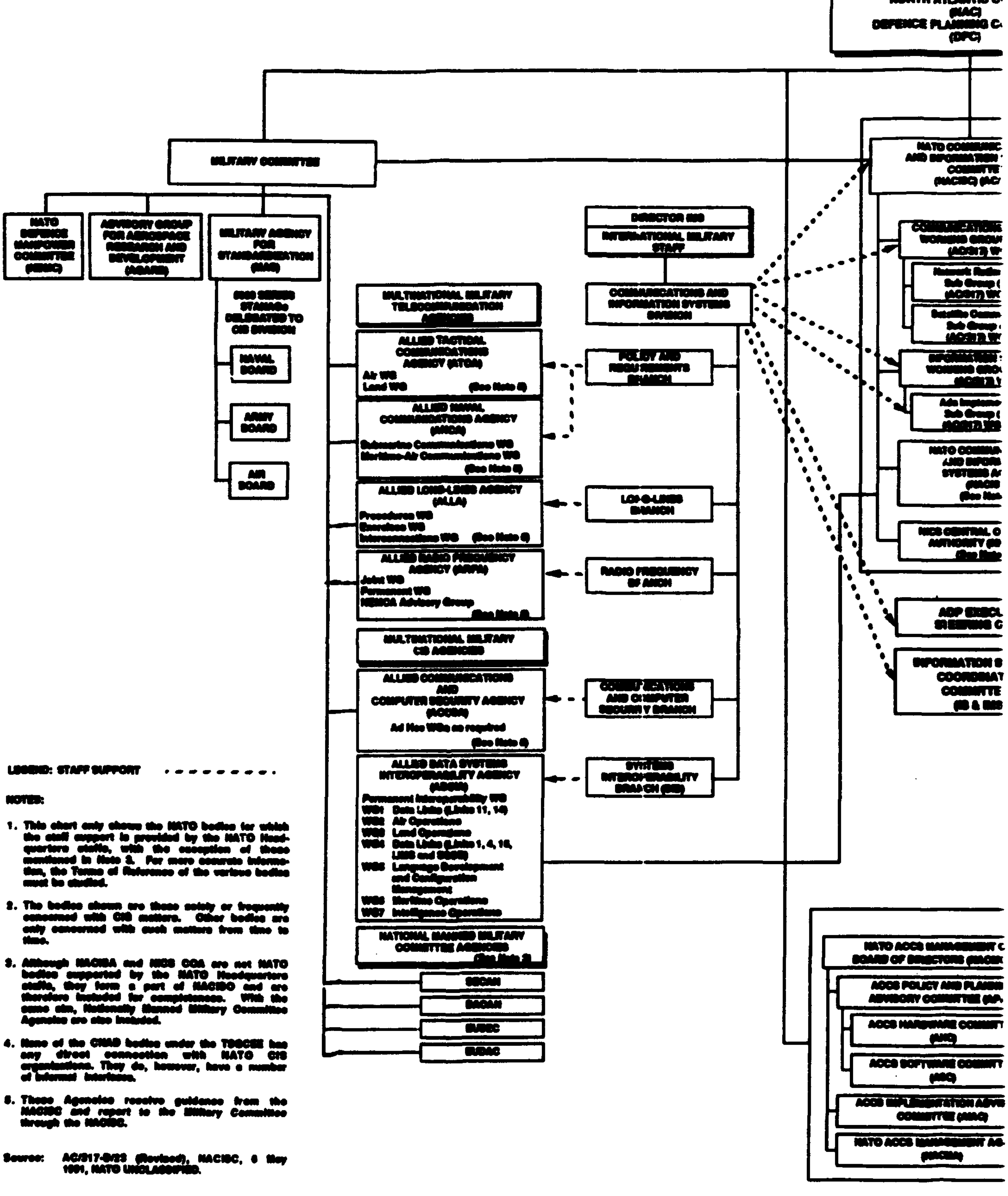
2.3 Standards Responsibilities of Selected NATO Bodies

Table F-2 is an incomplete first draft of an effort to identify the specific responsibilities of NATO organizations for technical standards. Eventually, this and similar tables for other groups of standards bodies will be analyzed to identify overlaps as well as possible gaps in the standards coverage. The following describes the areas of responsibilities for key NATO standards bodies [Ref. NIPD 1993]:

- The North Atlantic Council (NAC) and Defence Planning Committee (DPC) promulgate guidance that embraces interoperability, interdependency, and interfaces related to informatoin exchange in NATO.
- The NATO Standardization Group (NSG), directly reponsible to the NAC, is an independent body established to review the activities of all NATO bodies involved in the field of standardization, to include information system interoperability.
- The Military Committee (MC) is reponsible for the infrastructure-funded military subset of CCISs, which includes support for the MC itself at NATO headquaraters, the Major NATO Commmanders (MNCs), and the data interfaces between the various systems of NATO and the nations. The MC has relinquished its authority to the NACISC to provide the focus for communication and information system (CIS) interoperability and standardization for commor-funded systems.

---

4 *Working Relationships* [Ref. NACISC 1989c].



LEGEND: STAFF SUPPORT - - - - - - - - - -

NOTES:

1. This chart only shows the NATO bodies for which the staff support is provided by the NATO Headquarters staffs, with the exception of those mentioned in Note 3. For more accurate information, the Terms of Reference of the various bodies must be studied.

2. The bodies shown are those solely or frequently concerned with CIS matters. Other bodies are only concerned with such matters from time to time.

3. Although NACISA and NICS COA are not NATO bodies supported by the NATO Headquarters staffs, they form a part of NACISC and are therefore included for completeness. With the same aim, Nationally Manned Military Committee Agencies are also included.

4. None of the CNAD bodies under the TSGCEE has any direct connection with NATO CIS organizations. They do, however, have a number of informal interfaces.

5. These Agencies receive guidance from the NACISC and report to the Military Committee through the NACISC.

Source: AC/317-D/23 (Revised), NACISC, 6 May 1991, NATO UNCLASSIFIED.

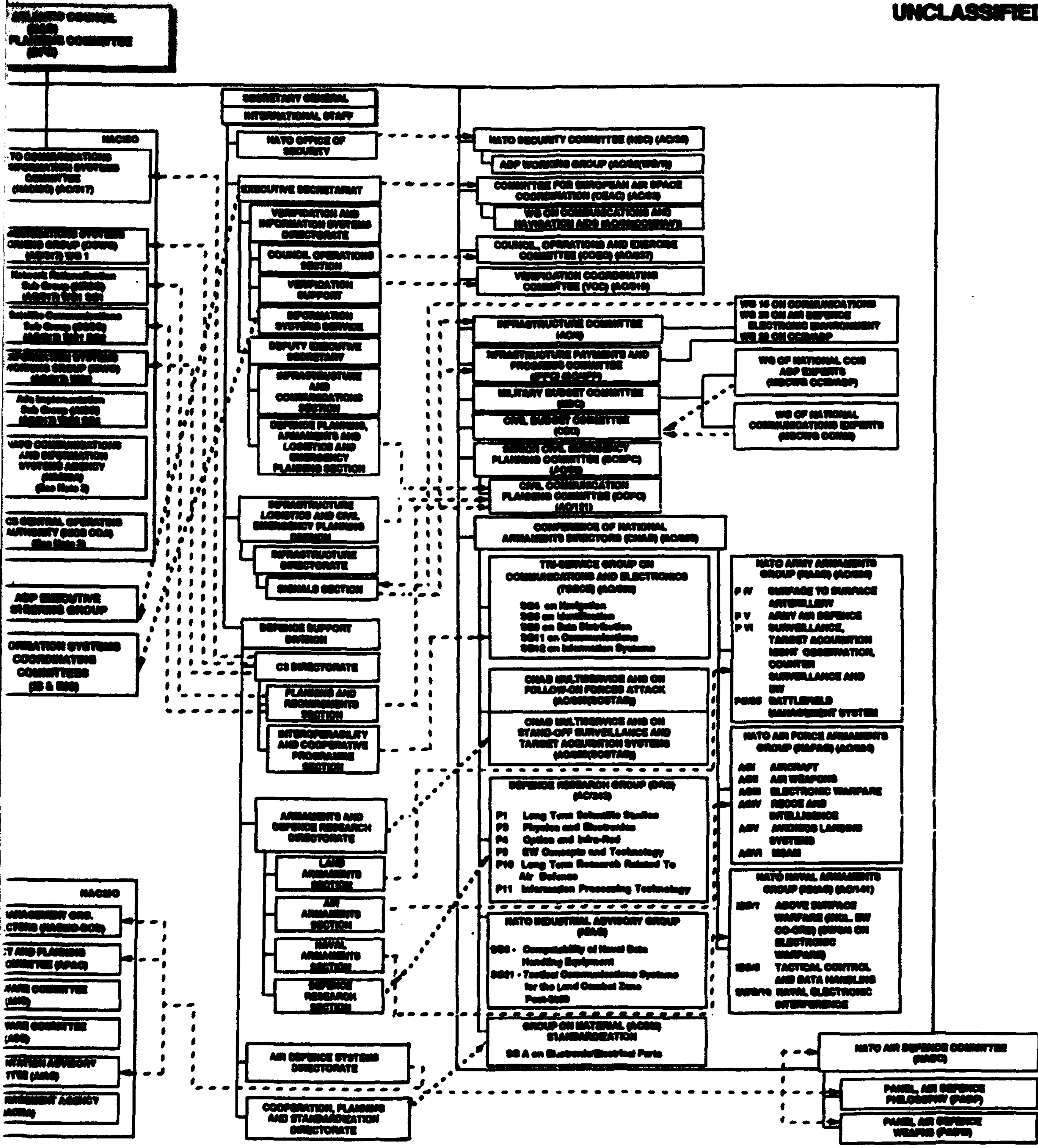


Figure F-1. NATO Bodies in the Fields of Communications and Information Systems

2

- The task of the Military Agency for Standardization (MAS) is to foster military standardization within the policy established by the MC with the aim of enabling the NATO forces to operate effectively together. The MAS is responsible for the NATO-wide coordiantion and validation of tactical IERs and the development and maintenance of operational interoperability standards. The MAS initiates, promulgates, and maintains STANAGs and Allied publications.
- Allied Tactical Communications Agency (ATCA) and Allied Naval Communications Agency (ANCA) are reponsible to the MC for development of military telecommunications policy, concepts, plans, requirements, and procedures to ensure an effective telecommunications capability for tactical land and/or air operations (ATCA) and maritime operations (ANCA).
- Allied Communications and Computer Security Agency (ACCSA) is responsible for satisfying peace- and wartime-NATO and NATO-related national requirements concerning communications security and computer security matters.
- ARFA is responsible for satsifying peace- and wartime-NATO and national radio frequency reqauirements.
- NATO Communications and Information Systems Committee (NACISC) provides the focus for CIS interoperability and standardization for common funded systems. It is tasked iwth specifying the procedures regarding the form in which information is transferred, standard reporting language, and operational procedures appropriate to NATO CCISs and associated data links.
- NATO Communications and Information Systems Agency (NACISA) provides central technical planning and designs the systems engineering and configuration management for NATO CISs. It also provides guidance on the implementation of standards and their application in national systems.
- The Communications Systems Working Group (CSWG—WG1) and the Information Systems Working Group (ISWG—WG2) are subordinate bodies of the NACISC, responsible for NATO procedural interoperability standards with respect to communications other than tactical data links (CSWG) and the formulation of plicy issues with special consideration for interoperability requirements (ISWG).
- The Allied Data Systems Interoperability Agency (ADSIA) is a multinational military CIS agency reponsible to the NACISC principally for coordinating the overall development and configuration management of NATO common interoperability standards, except those under the purview of the CSWG.
- The Conference of National Armaments Directors (CNAD) acts under direct authority of the NAC and advise the NAC on matters pertaining to the development and procurement of defense equipment for NAT forces and connected problems. In the field of CIS interoperability, the CNAD is primarily responsible for NATO technical interopeability standards.
- Tri-Service Group on Communications and Electronics (TSGCE) actively promotes and enables collaboration among nations of the Alliance on projects to develop, test, produce, and procure common equipment and systems in order to minimize cost and ensure full interoperability; and to develop and perform configuration management of technical standards in oder to promote greater interoperability in NATO and national systems.
- Three armaments groups subordinate to the CNAD promote cooperation in developing and producing weapon systems and equipment: NATO Army Armaaments Group (NAAG), NATO Air Force Armaaments Group (NAAFG), and NATO Navy Armaaments Group (NNAG).
- The NATO Air Defence Committe (NADC) comprises Air Defence Representatives (ADREPs) to provide a form for an exchange of views on the continuing development of the air defense program. Advice is provided to the NADC from the Panel on Air Defense Philosophy (PADP), whcich addresses possible consequences for capabilities and proposals, and the Panel on Air Defence Weapons, which assists in the development of a coherent air defense system and identifies opportunities for and participates in collaboration in air defnese weapons research, development, and production.
- The NATO Air Command and Control Agency (NACMA) is responsible for the Air Command and Control System (ACCS) development. The parent body of NACMA is the NATO ACCS Management Organization Board of Directors (NACMO BOD).

Table F-1. Acronyms and Titles of Key NATO Bodies in the Fields of Communications and Information Systems Standardization

Acronym	Name
NAC	North Atlantic Council
NSG	NATO Standardization Group
DPC	Defence Planning Committee
MC	Military Committee
AGARD	Advisory Group for Aerospace Research and Development
MAS	Military Agency for Standardization
MNCs	Major NATO Commands
ACE	Allied Command Europe
CHAN	Allied Channel Command
LANT	Allied Command Atlantic
ATCA	Allied Tactical Communications Agency
ANCA	Allied Naval Communications Agency
ALLA	Allied Long Lines Agency
ARFA	Allied Radio Frequency Agency
ACCSA	Allied Communications and Computer Security Agency
ADSIA	Allied Data Systems Interoperability Agency
SECAN	Communications Security and Evaluation Agency
DACAN	Distribution and Accounting Agency
EUSEC	European Security and Evaluation Committee
	European Distribution and Accounting Agency
IMS	International Military Staff
CIS DIV	Communications and Information Systems Division
NACISO	NATO Communications and Information Systems Organization
NACISC	NATO Communications and Information Systems Committee
CSWG	Communications Systems Working Group
NRSG	NATO Rationalization Subgroup
SCSG	Satellite Communications Subgroup
ISWG	Information Systems Working Group
AISG	Ada Implementation Subgroup
NACISA	NATO Communications and Information Systems Agency
NICS-COA	Central Operating Authority
CNAD	Conference of NATO Armaments Directors
TSGCEE	Tri-Service Group on Communications and Electronic Equipment
NAAG	NATO Army Armaments Group
NAFAG	NATO Air Force Armaments Group
NNAG	NATO Navy Armaments Group
DRG	Defence Research Group
NIAG	NATO Industrial Advisory Group
CEAC	Committee for European Airspace Coordination
NADC	NATO Air Defence Committee

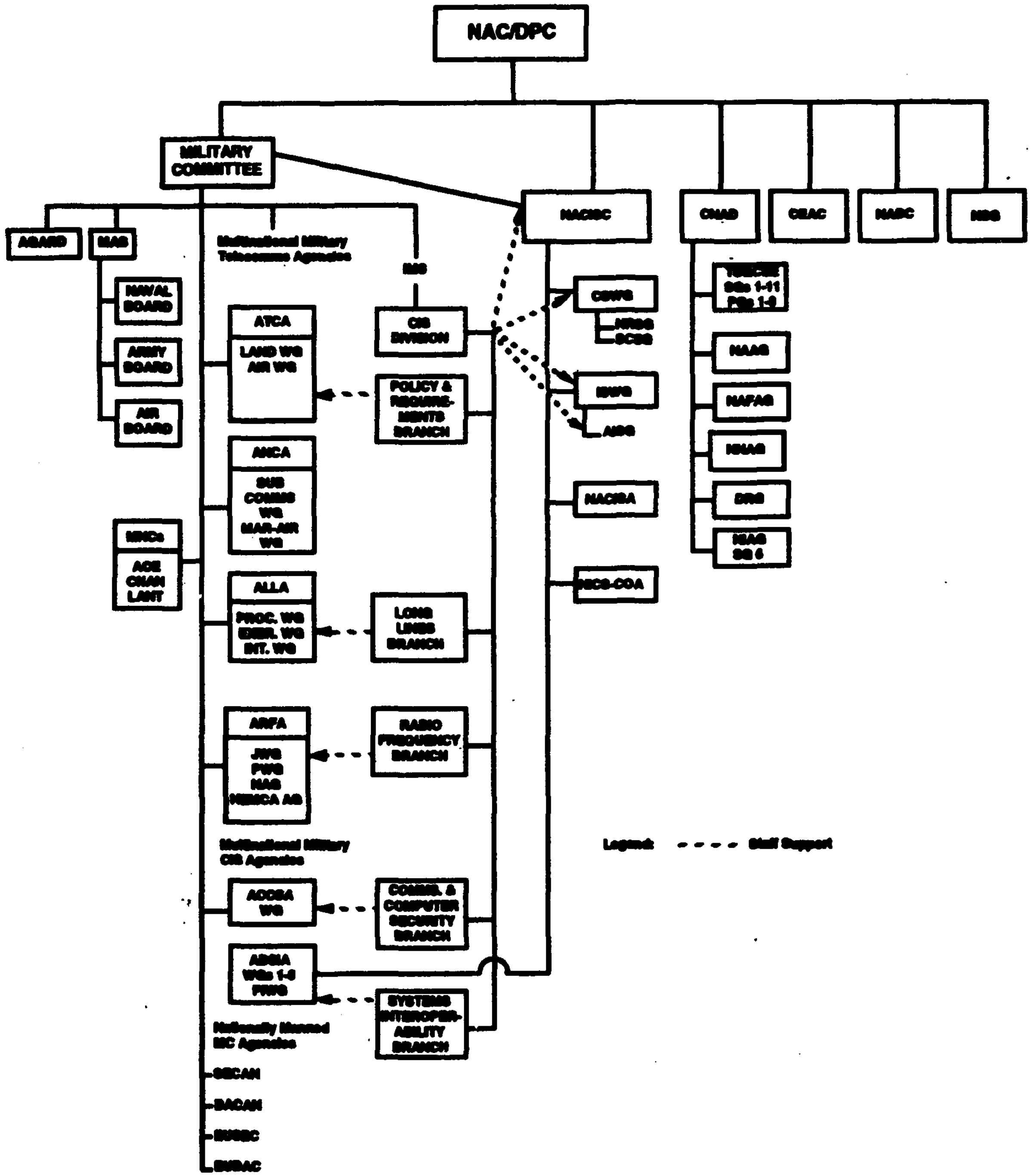


Figure F-2. NATO Standards Bodies for Communications and Information Systems

Table F-2. Responsibility for Standards in NATO Bodies

NATO Organization	Title	Standards Responsibility
CNAD	Conf of Nat'l Armaments Directors	
TSGCEE	Tri-Serv Group Comm-Electron Equipment	Technical Standards
SG1	Tactical Area Communications	STANAGs 4206-4214,4249,4290,4295,5000-5018
SG2	Tactical Radio Equipment	STANAGs 4197-4205,4245-46,4285-92,4335-39,5020
SG3	Multi-Functional Info Distribution	
SG4	Navigation and Position Finding	
SG5	Identification	
SG7	Channel Eval Tech in HF Communications	
SG8	Tactical SATCOM Terminal	STANAGs 4231-33, 4271
SG9	Data Processing and Distribution	NATO OSI Standards; STANAG 4250
AHWG-Security	OSI Security	NATO OSI Standards (Annex B)
AHWG-OM	OSI Network Management	NATO OSI Standards (e.g., Net Mgmt)
AHWG-ISDN	Integrated Services Digital Network	ISDN Standards for Open Systems
WG1	Lower 4 Layers of Reference Model	STANAGs 4251-54, 4261-64
WG2	Upper 3 Layers of Reference Model	STANAGs 4255-56, 4258-59, 4265-66
AHWG-MMHS	Military Msg Handling System	STANAG 4257
WG3	Comm System/Network Interoperability	MOU for Multinational Programme
SG10	Geographic Information	
PG2	NATO Identification System	
PG3	MIDS	
PG4	Low Cost INS for Ships	
PG5	Multi-Functional Inertial Sensor Assembly	
PG6	Tac Comm Post 2000-Land Combat	
PG7	BICES	
PG8	Tactical Spectrum Mgmt System	
CGN	Conformance Testing	
NIAG	NATO Industrial Advisory Group	
SG6	Naval Data Handling Equipment	Functional Profiles
NACISC	NATO Comm and Info Sys Committee	Oversight for Procedural Standards
CSWG	Comm Systems Working Group	
ISWG	Information Systems Working Group	
AISG	Ada Implementation Subgroup	
NACISA	NATO Comm and Info Sys Agency	
NICS-COA	Central Operating Authority	
MC	Military Committee	
IMS	International Military Staff	
CCCS Div	Command, Control and Comm System	STANAGs 5000-6999
CISD	Comm and Info Systems Divison	
SIB	Systems Interoperability Branch	
MAS	Military Agency for Standardization	Operational Standards (STANAGs 1000-3999)
Air Board	Air Board	STANAGs 8000-8999
ACCSA	Allied Comm and Comp Sec Agency	
PSN WG	Packet Switched Network	
ADSIA	Allied Data Systems Interop Agency	Procedural Standards
PIWG	Permanent Interoperability WG	
WG1	Maritime TDS Interoperability Standards	Data Links 10, 11, and 14
WG2	Air Operations	
WG3	Land Forces TDSs	
WG4	Inter-Service Data Systems	Data Links 1,16; LIMS,SSSB; STANAG 5516
WG5	Character-Oriented	Language Development and Configuration Mgmt
WG6	Maritime Operations	
WG7	Intelligence Operations	Intelligence Messages
WG8	Common Operational Vocabulary	
SECAN	Comm Security and Eval Agency	
NSG	NATO Standardization Group	Prepare Composite NATO Standardization Programme

3. INTERNATIONAL STANDARDS BODIES

Table F-3 identifies standards bodies such as ITU-TS, ISO, and ECMA that recommend, develop, and maintain technical standards for communications and information processing. The primary international bodies are described below.[5] National standards bodies are identified in Chapter 4 of this appendix.

Table F-3. Responsibilities for Communications and Information Processing in International Civil Standards Bodies

International Organization	Title	Standards Responsibility
ITU-TS (formerly CCITT)	International Telecommunications Union - Telecommunications Standards Sector	
SG 1	Service Definition	
SG 2	Network Operation	
SG 3	Tariff and Accounting Principles	
SG 4	Network Maintenance	
SG 5	Protection Against Electromagnetic Effects	
SG 6	Outside Plant	
SG 7	Data Networks and Open System Communications	OSI standards; facilities, interfacess
WG 1	Network Services, Facilities Prototypes	
WG 2	Network Access Interfaces	
WG 3	Internetworking, Switching, Signal	
WG 4	Transmission and Message Handling	
WG 5	Routing, Numbering, Layered Model	
SR ISDN	ISDN-Related Issues	
R DEFS	Terms and Definitions	
SG 8	Terminals for Telematic Services	OSI standards; FAX, teletex, videotex
WG 1	Terminal Characteristics	
WG 2	Common Protocols & Internetworking	
SG 9	Television and Sound Transmission	
SG 10	Languages for Telecommunications Applications	
SG 11	Switching and Signaling	
SG 12	End-to-end Transmission Performance of Networks and Terminals	
SG 13	General Network Aspects	
SG 14	Data Transmission over the Telephone Network	
SG 15	Transmission Systems and Equipment	
ITU-TDS (formerly CAR)	ITU - Telecommunication Development Sector	—
CEN	European Committee for Standardization	—
CENELEC	European Committee for Telecommunications Standardization	—
CEPT	European Conference of Postal & Telecom Administration	—
CCH	Harmonization Coordination Committee	
CAC	Commercial Action Committee	
CLTA	Liaison Committee for Transatlantic Telecommunications	
ECMA	European Computer Manufacturing Association	
TC29	Text Preparation & Interchange	Telematic services; text/office systems

5 "La Galaxie de la Normalisation" [Ref. Telecoms 1989]; *The OMNICON Index of Standards for Distributed Information and Telecommunication Systems* [Ref. OMNICON 1987]; and *The Value and Use of IT Standards in Public Procurement* [Ref. CEC 1988].

Table F-3. Responsibilities for Communications and Information Processing in International Civil Standards Bodies (Cont'd)

TC32	Communications, Networks & Systems Interconnection	OSI standards
TG1	Public Data Networks	
TG3	Local Area Networks	
TG6	Interfaces to Private Switching Networks	
TG7	Transport & Network Layers	Layer 3 and Layer 4 OSI standards
COS	Corporation for Open Systems	Testing
COSINE	Corporation for Open Systems in Europe	—
EMUG	European MAP User Group	—
ETSI	European Telecommunication Standards Institute	—
EWOS	European Workshop on Open Systems	Profiles
ISO	International Organization for Standardization	
JTC1 (TC97)	Technology Committee on Information Processing Systems	Promote standards worldwide
SGFS	Special Group on Functional Standardization	ISPs
SWG-API	Applications Programming Interface (as of August 1993, SWG-API has been dissolved) [Ref. SC21 N 8081 1993]	
SWG-CA	Conformity Assessment (as of August 1993, SWG-API has been dissolved) [Ref. SC21 N 8081 1993]	
SWG-EDI	Electronic Data Interchange	
SWG-MF	Modeling Facilities (Note that as of August 1993, SWG-MF has been dissolved) [Ref. SC21 N 8081 1993]	
SWG--P	Procedures	
SWG-RA	Registration Authorities	
SWG-SP	StrategicPlanning	
SC1	Vocabulary	
SC2	Character Sets & Information Coding	
SC6	Telecommunications and Info Exchange Between Systems	
WG1	Data Link Layer	
WG2	Network Layer	
WG3	Physical Layer	
WG5	Transport Layer	
WG6	Private Integrated Services Networking	
SC7	Software Engineering	
WG1	Symbols, Charts, and Diagrams	
WG2	System and Software Documentation	
WG4	Tools and Environments	
WG5	Reference Model for Software Development	
WG6	Evaluation and Metrics	
WG7	Life Cycle Management	
WG8	Integral Life Cycle Processes	
WG9	Classification and Mapping	
SC11	Flexible Magnetic Media for Digital Data Interchange	
SC14	Data Element Principles	DE standardization
WG4	Coordination of Data Element Standardization	
SC15	Labeling and File Structure	
SC17	Identification and Related Devices	
SC18	Document Processing and Related Communication	Message Handling Protocols
WG1	User Requirements	
WG3	Office Document Architecture and Interchange Format	ODA/ODIF
WG4	Procedures for Text Interchange	MOTIS
WG5	Content Architectures	
WG8	Text Description and Processing Languages	
WG9	User System Interfaces and Symbols	
SC21	Open Systems Interconnection, Data Management and Open Distributed Processing	OSI and other standards
WG1	OSI Architecture	OSI architecture, reference model, security, QOS, conformance testing, LOTOS, Estelle

Table F-3. Responsibilities for Communications and Information Processing in International Civil Standards Bodies (Cont'd)

SC21	Open Systems Interconnection, Data Management and Open Distributed Processing	OSI and other standards
WG1	OSI Architecture	OSI architecture, reference model, security, QOS, conformance testing, LOTOS, Estelle
WG3	Database (not part of OSI)	SQL, IRDS, RDA, Data Management, Conceptual Schema
WG4	OSI Management and OSI Directory	CMIS, CMIP, systems management, SMI, managed objects, Directory
WG7	Open Distributed Processing (not part of OSI)	ODP, ODP Trader
WG8	OSI Upper Layers	Layers 5-7; ALS, XALS, ACSE, ROSE, RTSE, GULS, RPC, VT, FTAM, RPC, TP, TM, ASN.1
WG9	Testing	
SC22	Languages	
WG15	POSIX	
WG20	Internationalization	
SC23	Optical Disk Cartridges for Information Interchange	
SC24	Computer Graphics and Image Processing	Work formerly done by SC21/WG2
WG1	Architecture	
WG2	Application Programming Interfaces	
WG3	Metafiles and Device Interfaces	
WG4	Language Binding	
WG5	Validation, Testing, and Registration	
SC25	Interconnection of IT Equipment	
SC26	Microprocessor Systems	
SC27	Common Security Techniques for IT Applications	
WG1	Secret Key Algorithms and Applications	
WG2	Public Key Crypto-systems and Modes of Use	
WG3	Use of Encipherment Techniques in Communication Architectures	
SC28	Office Equipment	
IEC	International Electrotechnical Commission	—
IFIP	International Federation for Information Processing	—
ITSTC	Information Technology Steering Technology Committee	—
OSITOP	OSI for Technical & Office Protocol	—
OSF	Open Software Foundation	—
POSI	Promotion Conference for OSI	Asia-Oceania workshop/standards forum
SOGITS	Senior Official Group for Info Tech Standardization	Commission of European Communities
SOGT	Senior Official Group on Telecommunications	Commission of European Communities
SPAG	Standards Application & Promotion Group	—
UER	European Union on Radio Broadcasting	—
X/OPEN	X/OPEN	—

3.1 CEN/CENELEC

The Comite Europeen de Normalisation (CEN) is a grouping of the national organizations of 18 countries of the European Community (EC) and the European Free Trading Association (EFTA).[6] CEN works in

6 The EFTA is also known as the Association Europeenne de Libre Exchange (AELE).

cooperation with the Comite Europeen de Normalisation Electrotechnique (CENELEC) to develop and publish European standards [normes europeennes (ENs)]. CENELEC deals exclusively with electrotechnical standards and CEN works with standards in all other areas. Based in Brussels, CEN/CENELEC works to harmonize standards that are established by its members and to create European standards where no other appropriate standards exist. CEN/CENELEC members include AFNOR (France), UNI (Italy), DIN (Germany), BSI (United Kingdom), IBN (Belgium), DCQ (Portugal), and SIS (Sweden).

CEN/CENELEC standards are initially distributed for comment by member bodies in the form of an experimental standard (ENV[7]) or a European prestandard (prENV). Future technical work in developing proposals for ENVs has now been taken over by the European Workshop for Open Systems (EWOS). When proposed international standards are harmonized with national standards, harmonized documents (HDs) are produced. When adopted, an HD must be used and national deviations can only exist temporarily. European norms (ENs) must be adopted as national standards, and any conflicting national standards must be withdrawn. An example standard is ENV 41201, Private Message Handling System. A second class of standards promulgated by CEN/CENELEC are the Telecommunications European Norms (NETs), which are common technical specifications covering access to networks and equipment. Examples are NET2 (X.25 Access) and NET3 (ISDN Basic Access).

CEN/CENELEC standards originate as draft documents, standards proposals, and implementors guides developed by various standards promoting organizations. When stable, these documents are reviewed and coordinated by the European Telecommunications Standards Institute (ETSI) and EWOS and are issued for comment as functional specifications, recommendations, and technical specifications. When the review is complete, they are forwarded to CEN/CENELEC, or to the Conference Europeenne des Postes et Telecommunications (CEPT), for final standards development.[8]

3.2 CEPT/ETSI/UER

Three consortia represent the interests of public telecommunication administrations of European countries. The Conference Europeenne des Postes et Telecommunications (CEPT) coordinates political aspects and prepares technical specifications for member administrations (but does not produce any standards). The CEPT has 20 member countries and works closely with CEN/CENELEC. The European Telecommunications Standards Institute (ETSI) is an organization created within CEPT to prepare specifications concerning public telecommunications networks. The Union Europeenne de Radiodiffusion (UER) is a technical committee with the aim of harmonizing radio broadcasting system standards; its proposals are transmitted to the CCIR and the IEC. The UER has 32 countries actively participating and 45 associated member bodies.

3.3 Conference on Data Systems Languages (CODASYL)

Formed in 1960, the Conference on Data Systems Languages (CODASYL) has been active in the development of the COBOL language, a common Data Description Language (DDL) for defining schemata and subschemata and a data manipulation language.

3.4 Corporation for Open Systems (COS)/Corporation for Open Systems Interconnection Networking in Europe (COSINE)

The Corporation for Open Systems (COS) and the Corporation for Open Systems Interconnection Networking in Europe (COSINE) participate in the development of functional profiles for OSI and play an active role in setting standards for testing OSI products for conformance to the international standards and profiles. COS is based in Vienna, Virginia, in the United States, and COSINE is based in Paris.

COS has over 60 member organizations, both vendors and users. Its goal is to promote and accelerate the adoption of interoperable, multivendor products and services based on OSI and ISDN standards. To accomplish this goal, COS provides a user-vendor forum for the statement of user requirements and the discussion and management of the issues surrounding the deployment of open systems. COS also identifies test requirements and sponsors test-tool development and conformance and interoperability testing to verify that computer products and services conform to OSI and ISDN standards.

COSINE is a project established by the CEC to promote internetworking facilities between industrial and academic research and development communities throughout Europe. Participating countries are Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, the United Kingdom, and Yugoslavia.

One COSINE project was establishing a pan-European OSI data networking infrastructure for European research. COSINE is intended as an enabling or catalytic project, not a long-term operational activity. The Reseaux

---

7 The "V" in ENV is for "Vornorm," and indicates a standard based on DIS or other draft standards that are not completely stable; modifications to ENV standards may eventually be required to bring them in line with international standards. ENVs are valid for 3 years--they are reviewed after 2 years and may then become an EN, be prolonged for another 2 years, be replaced by another ENV, or be withdrawn.

8 *Briefing on EUROPE 92--The European Community's Approach to Integration in the Information Technology Area* [Ref. Griefenstein 1989].

Associes pour Recherche Europeene (RARE—Association of European Research Networks), which exists to coordinate and promote networking activities for the European research community, could add an operational or service role to its present representative, promotional, and coordinating functions and take over any activities from COSINE that remain necessary after the end of the project.[9]

3.5 Electric Power Research Institute (EPRI)

The Electric Power Research Institute (EPRI) is a US industry association of more than 670 publicly and privately owned utilities that is facilitating the use of open systems technology in the utility industry. It has developed a Utilities Communications Architecture (UCA) as a GOSIP-like profile. EPRI's specific interests span real-time UNIX, expert systems, and database access using RDA and SQL.

3.6 European Computer Manufacturer Association (ECMA)

The European Computer Manufacturer Association (ECMA) represents a group of 33 manufacturers in Europe. Its work is conducted by 14 technical committees. Based in Geneva, ECMA acts as an observer at ISO and as a consultant at ITU-TS. ECMA takes an active role in the definition of functional profiles with EWOS. ECMA contributes to the ISO standards development efforts, in addition to issuing its own standards. It is particularly active in the development of higher layer protocols for OSI networking and is developing a standard for a Portable Common Tool Environment (PCTE).

3.7 European Manufacturing Automation Program (MAP)

The European Manufacturing Automation Program (MAP) User Group (EMUG) was created in 1985 by a large group of manufacturers. It aims to promote the MAP standards in Europe. Specific groups in the nations, such as the Club Informatique des Grandes Enterprises Francaises (CIGREF) in France, are appointed to be EMUG's representatives. A key element of MAP, the Manufacturing Message Specification (MMS) has reached DIS status (DIS 9506).

3.8 European Strategic Programme for Research and Development in Information Technology (ESPRIT)

European Strategic Programme for Research and Development in Information Technology (ESPRIT) is a European research program initiative begun in 1982 and sponsored by the Commission on European Communities. Its major work areas are advanced microelectronics, software engineering and technology, advanced information processing, office automation, and computer integrated manufacturing. ESPRIT has contributed to many standards projects, such as PCTE, Communications Network for Manufacturing Applications (CNMA), and Herode, which has prepared an office document architecture standard for adoption by ISO. The future focus of ESPRIT will be on developing microelectronics and peripheral technologies, creating technologies and tools for the design of information processing systems, and enhancing the capacity for using and integrating information technology to extend the scope of its applications.

3.9 European Workshop on Open Systems (EWOS)

The European Workshop on Open Systems (EWOS) promulgates harmonized technical proposals for functional profiles of OSI standards and corresponding conformance test specifications. EWOS has been given the responsibility for technical work in developing proposals for ENVs, with increased involvement of users. When complete, the proposals are submitted to CEN/CENELEC. The founding members of EWOS include CEN, CENELEC, ECMA, EMUG, OSITOP, RARE, and the Corporation for Open Systems Interconnection Networking in Europe (COSINE). The member bodies of EWOS have agreed not to undertake on their own any new work on the development of functional standards. The focus is now on development of profiles (ISPs).

3.10 Information Technology Steering Technical Committee (ITSTC)

The Information Technology Steering Technical Committee (ITSTC) provides recommendations for European members in three areas: standards (the Information Technology Ad-hoc Expert Group for Standards), manufacturing/automation (the Information Technology Ad-hoc Expert Group for Manufacturing), and certification (the Information Technology Ad-hoc Expert Group for Certification). While the ITSTC does not produce standards, it does define programmes for European standards and organizes and coordinates the work.

3.11 International Federation for Information Processing (IFIP)

The International Federation for Information Processing (IFIP) is a group of international experts drawn principally from universities and also from some industries (e.g., Xerox, Bell). IFIP has contributed to the work of ISO on the OSI model and, more recently, to the work on X.400-type message handling systems.

9 "COSINE on Target for 1992" [Ref. OSN 1991a].

3.12 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)

The International Organization for Standardization (ISO) has 89 members representing national standards bodies (e.g., AFNOR in France, JISC in Japan, ANSI in the United States, BSI in the United Kingdom). The International Electrotechnical Commission (IEC)[10] is a federation of more than 200 national committees working in the area of electronics and electrical standards with specific interest in information processing. ISO and IEC have formed a joint committee, Joint Technical Committee One (JTC1), to develop standards for information processing systems.

3.13 Internet Activities Board (IAB)

The IAB is a committee of researchers and professionals that manages the technical standards and architecture of the Internet, a collection of more than 5,000 packet-switched networks world wide, 80 percent of which are in the United States To maintain uniformity within the network, IAB approves Internet Standards and manages the process by which they are published.

3.14 ISO Development Environment (ISODE) Consortium

The ISODE Consortium was formed in 1992 to take charge of further development of ISODE, a public-domain implementation of OSI, and "commercialize" it. The Consortium aims to position ISODE as a package on which vendors can build OSI products and to support its continued use in the research community. The Consortium is a professional non-profit corporation, the initial start-up of which was achieved by funding from the Microelectronics and Computer Technology Corporation (MCC) in Austin, TX. [Ref. OSN 1992o]

3.15 International Telecommunications Union - Telecommunication Standardization Sector (ITU-TS) (formerly CCITT/CCIR)

The International Telecommunications Union - Telecommunication Standardization Sector (ITU-TS) [formerly the Comite Consultatif International pour le Telephone et le Telegraph (CCITT) and International Radio Consultative Committee (CCIR)] is one of three sectors of the ITU, a United Nations treaty organization. The other two sectors are Radiocommunication and Telecommunication Development. The ITU groups all the Postal Telephone Telegraph (PTT) administrations of the world's countries. ITU-TS develops standards in 4-year cycles and works closely with ISO to harmonize results. It is based in Geneva.

ITU-TS's primary mission is to develop standards supporting the international interconnection and interoperability of telecommunications networks at interfaces with end-user systems, carriers, information and enhanced-service providers, and customer premises equipment. Its recommendations are mandatory in Europe where communications are nationalized.

3.16 Message-Oriented Middleware Consortium (MOM)

The Message-Oriented Middleware Consortium (MOM) [Ref. Stahl 1993] is a new middleware-vendor association (see Section 13.5). MOM promotes middleware that uses messaging technology to allow applications to communicate across distributed platforms. Consortium members include Digital Equipment, IBM, and Covia Technologies. The intent of the consortium is to create standards in messaging middleware.

3.17 National Information Infrastructure Testbed (NIIT)

The National Information Infrastructure Testbed (NIIT) is a consortium of representatives from US industry, academia, and government that was formed in September 1993 to leverage the National Information Infrastructure (NII) vision and principles. NIIT will implement the vision of the NII through the development of distributed applications requiring the speed and transmission capacity of a true data superhighway system.

3.18 National Protocol Support Center (NPSC)

An Australian organization, the National Protocol Support Center (NPSC) was formed in 1986 as a joint effort between industry and government to promote the adoptions of OSI standards in formation technology and to support conformance testing capabilities in Australia.

3.19 Network Management Forum (NM Forum)

The NM Forum is an international consortium aiming to accelerate and promote international standards for network management. The Forum does not create products or standards, but instead specifies interfaces and profiles that promote the use of standards among vendors. Originally launched in 1988 as the OSI Network Management Forum, the group became the NM Forum in 1990 reflecting its inclusive attitude to management standards. It is developing a roadmap (EWOS/TZ/91/214) that is an industry-accepted, standards-based concept that promotes product interoperability. The Roadmap plan is a path consisting of a series of points in time (OMNIPoints). At each point

---

[10] The IEC is also known as the Commission Electrotechnique Internationale (CEI).

it is agreed that it is sensible to build interoperable management products to agreed interfaces with agreed functionality. [11]

3.20 Object Management Group (OMG)

OMG specifies standard interfaces for object-oriented software. It was formed in April 1989 by 9 companies and now has more than 145 member organizations comprised of vendors, software developers, and users. It aims to establish a framework and supporting specifications for commercially available object-oriented environments. It has created a reference model, the Object Management Architecture. OMG's object request broker design–key software needed to allow disparate open systems to request object services from remote sites–is commonly supported by object-oriented software vendors.

3.21 Open Document Architecture Consortium (ODAC)

Six major international computer companies formed the Open Document Architecture Consortium (ODAC) in early 1991 to develop a toolkit of software that conforms to the ISO ODA standard. The toolkit will be openly licensed to allow other computer companies and systems developers to build software applications using ODAC's published specifications. It is expected to be available in 1993. The consortium members are currently: Digital, ICL, Siemens Nixdorf Informationsysteme, Groupe Bull, IBM, and Unisys. The Consortium has been established as a European Economic Interest Group in Brussels. [Ref. OSN 1991b, 24]

3.22 Open Software Foundation (OSF)

Created in 1988, the Open Software Foundation (OSF) is a nonprofit, international consortium of over 90 information systems companies (including International Business Machines) for the promotion of standards, such as the POSIX standard for operating system interfaces. Its goals include the development of software specifications and test suites for an open computing environment. OSF specifications are defined, and software developed, using an open process into which vendors and users have input and access. The resulting AES specifications are available in the public domain and its software licensable. Both members and nonmembers can submit technologies for consideration as an OSF specification or offering through a request for technology (RFT) process. OSF's specifications and software are based on POSIX, a variety of international, national, and industry standards and other consortia specifications.

3.23 Open Systems Testing Consortium (OSTC)

Members of the OSTC provide third party OSI conformance testing for wide area networking products at a number of test laboratories throughout Europe. It is an international organization encompassing PTTs, public network operators, manufacturers, and research organizations.

3.24 OSI Multipeer/Multicast (MPMC) Consortium

The OSI MPMC Consortium has been formed under the National Science Foundation's Industry/Academia Cooperative Research Program at North Carolina State's Center for Communications and Signal Processing. The Consortium presently has three subscribing members: the DoD DISA/JIEO, the US Army's Project Manager for Training Devices, and the US Army Communications-Electronics Command Software Engineering Directorate. Four academic institutions (University of Delaware, University of New Hampshire, University of Central Florida, and North Carolina State University) are presently participating and contributing to the research and progression of the MPMC work, and two consultants (Open Network Solutions and the MOSAIC Group) are progressing standards development under previously existing projects. The goal of the consortium is to produce standardized MPMC communications environments with cooperative/leveraged resources of the interested and benefiting parties. The areas it plans to address include standards, progression, formal specifications, PICS Proforma, conformance and interworking testing, MPMC testbed, OSI MPMC network, and performance-cost tools. In addition, it will conduct fora three times per year.[12]

3.25 OSINET

OSINET was formed in 1984 under the auspices of NIST. Governed by its membership it works in three specific areas: (1) the research and development of test scripts that are used in OSI interoperability testing, (2) the interoperability testing and registration of announced OSI products, and (3) the demonstration and promotion of ISO technology. The US-based organization comprises 55 members and recently voted to reorganize under the auspices of COS [OSN 1991b, 23].

3.26 OSITOP

Open Systems Interconnection for Technical and Office Protocol (OSITOP) is an association of users (such as BNP, EDF/GDF) for the promotion of ISO functional profiles and the concept of TOP.

---

11 "A Roadmap for Open Management" [Ref. OSN 1992e].

12 *Open Systems Interconnect (OSI) Multipeer/Multicast (MPMC) Prospectus* [Ref. MPMC 1991].

3.27 PCTE Interface Management Board (PIMB) Association

The PCTE Interface Management Board (PIMB) Association is a non-profit international company whose purpose is to promote greater use of the PCTE interface and to encourage development of tools and software engineering methodologies using PCTE. It was established in May 1992 but has its origin within the PIMB, an informal group formed in October 1986 to coordinate standardization and exploitation of several PCTE-based ESPRIT (European Strategic Programme for Research into Information Technology) projects. Since 1986, PIMB has grown to 35 companies worldwide, including IT users, tool suppliers, computer manufacturers, software companies, and PCTE environment suppliers. [Ref. Vernocchi 1992]

3.28 Petrochemical Open Software Corporation (POSC)

Petrochemical Open Software Corporation (POSC) was founded in 1990 by a group of major oil companies to facilitate the development of integrated computing technology for the exploration and production segment of the international petroleum industry. Membership now includes exploration and production service companies, software vendors, computer manufacturers, and research institutes. POSC is focusing on the development of an industry-standard, open-systems-based, software-integration profile for exploration and production applications that will define common interfaces between software applications, database management systems, workstations, and users. This work includes development of an integrated data model, a common look and feel for user interfaces, and a set of test suites.

3.29 Promotion Conference for Open Systems Interconnection (POSI)/INTAP

Created by six major vendors in Japan and the Nippon Telephone and Telegraph (NTT) Corporation, the Promotion Conference for Open Systems Interconnection (POSI) is the equivalent to SPAG in Europe and to COS in the United States. POSI is an Asia-Oceania regional forum for the international workshops on OSI, and as such, seeks agreements among vendors to ensure interoperability and compatibility of products. The POSI regional workshop is known as the Asia-Oceania Workshop (AOW).

POSI will use the conformance testing tools and services developed by the Interoperability Technology Association for Information Processing (INTAP). INTAP is a national agency of Japan, funded by MITI, that deals with information technology, specifically OSI products and advanced projects.

3.30 SQL Access Group (SAG)

The SAG is a non-profit corporation set up by vendors and users to develop technical specifications, including APIs, to enable multiple relational databases and application tools to work together using the SQL standard. Its goals are to define a common subset of SQL functions (e.g., SQL data format, protocols for moving data within a multivendor environment) in order to reconcile the many SQLs that exist and to specify an enhanced SQL programming interface that will let developers write a single application that can access a variety of SQL databases.

3.31 Standards Application and Promotion Group (SPAG)

The Standards Application and Promotion Group (SPAG), based in Brussels, was created in 1983 by 12 major European manufacturers (e.g., Bull, ICL, Siemens) and now includes about 65 information technology manufacturers and users. SPAG's goals are to promote multivendor, interoperable products based on international standards, particularly OSI, and to keep its members informed about the latest developments in functional standards and conformance testing of products. SPAG seeks to accelerate standardization by selecting, among all OSI standards, a limited number for implementation. The stacks of standards are called profiles and are developed toward supporting complete applications, such as FTAM. SPAG has made a major contribution to the rapid progress of European experimental standards (ENVs) and standards (ENs). It plays a leading role in EWOS, regularly publishes the Guide to the Use of Standards, and participates in development of ISPs. However, an August 1993 article states that the future of SPAG is in the balance thanks to the slow take-off of OSI and the world recession. Following warnings from sponsors that funding could not be guaranteed next year, SPAG's director must drum up outside business before the end of the financial year, or lay off staff. [Ref. OSN 1993o]

3.32 Support to the Commission of the European Community (CEC)

The Senior Official Group for Information Technology Standardization (SOGITS) and the Senior Official Group on Telecommunications (SOGT) assist the CEC in the implementing legislation for information technology standards. The Public Procurement Subcommittee in the Information Technology Sector (PPSC-IT) enforces the role of standards in public procurement for the CEC.

3.33 UNIX International (UI)

UI is a product-specific open systems organization, but it does not sell or license any software products itself. It directs the development of UNIX System V and related products, the majority of which are developed and sold by UNIX System Laboratories, a partly owned subsidiary of AT&T, the originator of UNIX. UI was formed in 1988 and claims 225 members. In late 1992, it was sold to Novell.

3.34 X.400 API Association (APIA)

APIA, formed in 1989, is a group of more than 20 computer and communications vendors working to facilitate the transfer of messages between all electronic message systems, specifically for use on local area networks of personal computers, through development and promotion of practical interfaces based on the ITU-TS's X.400 recommendations. The APIA is working to develop interfaces to message handling systems for use by a variety of applications such as gateways to other messaging systems, EDI, etc. In conjunction with X/Open, APIA completed in 1990 an X.400 API specification. It has also contributed to the IEEE P1224 standard.

3.35 X/Open

X/Open is an independent, non-profit consortium formed in 1984 to determine user and market requirements and to specify a complete, source-level-portable application environment and test suites. Although its members were initially vendors, its membership now encompasses users, system integrators, value-added resellers, government agencies worldwide, other industry-standards groups, and academic and research organizations. X/Open is developing extensions to UNIX SVID operating system standards to support a distributed transaction processing environment that meets OSI standards. X/Open is developing a Common Applications Environment—which includes specifications for an operating system interface, networking, data management, programming languages, floppy disk formats, internationalization, and distributed transaction processing—to promote software portability. Alignment of both activities with the emerging POSIX standards is planned.

4. NATIONAL STANDARDS BODIES

This section identifies national standards bodies and their responsibilities for standards development or use.[13] Additional contributions to this section would be welcomed.

4.1 Belgium

The Institut Belge de Normalisation (IBN) is the primary standards body for Belgium.

4.2 Canada

The Canadian Standards Association (CSA) is responsible for the development of OSI standards in Canada. The Standards Council of Canada (SCC) is a Canadian national non-governmental agency that develops standards policy. The SCC provides coordination and support for the National Standards System (NSS) and supports Canada's participation in international standards work.

4.3 Denmark

Danish Standards Association (Dansk Standardiseringsrad) is the ISO member body from Denmark. It is also the member body for CEN.

4.4 France

The Association Francaise de Normalisation (AFNOR) is the French official organization for normalization/standardization and the French member body for ISO. It works with manufacturers, users, and administration. It promulgates international standards in France, chooses working groups in which France is to take an active part, manages French technical experts, and defines/coordinates the proposals they must put forward in discussions. The AFNOR role also includes giving information--it sends out literature on national and international standards and answers questions from manufacturers and users. AFNOR standards are classified according to the activity to which they relate. For example, Class Z corresponds to data processing. The Union Technique de l'Electricite (UTE) is the member of CENELEC from France and an active participant in AFNOR for the development and exploitation of standards for electricity and electronics.

4.5 Germany

The Deutsches Institut fur Normung (DIN) is the official organization for standardization for the Federal Republic of Germany and Berlin (West) and is the member body of ISO and CEN.

4.6 Netherlands

The Nederlands Normalisatie-Instituut (NNI) is the ISO member body for the Netherlands. When ISO or ITU-TS standards are translated or modified, they are issued by NNI as NENs. For example, NEN-ISO 3309 is a translation of an ISO HDLC standard.

4.7 United Kingdom

The British Standards Institute (BSI) is the UK member of ISO and the recognized body for the preparation and promulgation of British national standards.

4.8 United States

The American National Standards Institute (ANSI) is the US member of ISO and a U.S. clearinghouse for voluntary standards.

Table F-4 identifies ANSI and other standards bodies[14] in the United States, both civil and military, that recommend, develop, manage, and maintain technical standards for communications and information processing.

Table F-5 identifies all the current Technical Committees (TCs) currently active in ANSI for Information Processing Systems (X3).

In the United States, the process of defining standards is voluntary and is coordinated by ANSI. ANSI accredits organizations such as professional and technical societies, trade associations, or consumer and labor groups to develop or adopt standards in various areas. Three types of organizations can create a standard: (1) Accredited Sponsor (AS), (2) Accredited Organization (AO), and (3) Accredited Standards Committee (ASC) [Ref. Cargill 1989].

---

13 *The OMNICON Index of Standards for Distributed Information and Telecommunication Systems* [Ref. OMNICON 1987].

14 Similar tables need to be developed for standards bodies in other nations. Additional contributions will be included in future editions of this working paper.

Table F-4. Responsibilities for Communications and Information Processing in US Standards Bodies[15]

Organization	Title	Standards Responsibility
ANSI X3	Information Processing	
X3S3	Technology Committee (TC) on Data Communications	Devel of US OSI standards; input to ISO JTC1/SC21
X3S3.1	Task Group on Data Communications Planning	General standardization efforts
X3S3.2	Task Group on Communications Vocabulary	Data transmission vocabulary
X3S3.3	Task Group on Network Layer	Directory, management, routing, ISDN
X3S3.4	Task Group on Control Procedures	Protocols, procedures, & management; X.25
X3S3.5	Task Group on Communications Systems Performance	Nomenclature, presentation & performance measurement
X3S3.7	Task Group on Public Data Network Access	ISDNs, gateways (X3.100, X.25, X.75, X.32)
X3T2	Technology Committee on Data Interchange	
X3T3	Technology Committee on ODP	
X3T4	Technology Committee on Security Techniques	
X3T5	Technology Committee on OSI	Development of US OSI standards; input to ISO JTC1/SC21
X3T5.1	OSI Architecture; Reference Model	FDTs; Conf Testing; Sec, Open Distributed Proc
X3T5.4	Task Group on OSI Management Protocols	Management, MIS, directory service
X3T5.5	Presentation and Application Layers	CL mode, VT, ASN.1
X3T5.7	Task Group on OSI Security Techniques	
X3T6	Task Group on Non-Contact Information Systems Interface	
X3T7	Internationalization	
X3T8	Fault Tolerance	
X3T9	Technology Committee on I/O Interface	
X3T9.2	Task Group on Lower Level Interface	
X3T9.3	Task Group on Device Level Interface	
X3T9.5	Task Group on Local Distribution Data Interface	
X3V1	Office and Publishing Systems	
X3V1.1	Task Group on User Requirements M.S.T.	
X3V1.3	Task Group on Document Architecture	
X3V1.4	Task Group on Text Interchange	
X3V1.5	Task Group on Content Architecture	
X3V1.8	Task Group on Text Description and Process Language	
X3V1.9	Task Group on User Systems Interface/Symbols	
X3V1.10	Task Group on Font Resources	
USCCITT	US Organization for CCITT (now called ITU-TS)	
NC	National Committee	
GS-A	Telecommunication Policies & Services	
SG-B	WATTC-1988	—
SG-C	Worldwide Telephone Network	
SG-D	Data and ISDN	
JWP	Joint Working Party on ISDN	
IEEE	Institute for Electrical and Electronic Engineering	
610	Computer Terminology	
802	Committee on Local Area Networks	
P1003	POSIX	—
P1201	Graphical User Interfaces	
SCWUI	Steering Committee on User Interface	
DSSC	Distributed Services Steering Committee	
PSC	Profile Steering Committee	

15 Updated from *X3 Projects Manual X3/SD-4*, July 1993 [Ref. ANSI 1993].

Table F-4. Responsibilities for Communications and Information Processing in US Standards Bodies (Cont'd)

COS	Corporation for Open Systems	Promote OSI; conformance testing
X/OPEN	X/OPEN	Promote portability and use of OSI
NIST	National Institute for Standards & Technology	Standards development and coordination; conformance
Workshops	Implementation Workshops	Develop design-to functional profiles
ASD(C3I)	Asst Sec Def C3I	
DASD C3	Deputy Assistant Secretary of Defense C3	
T&TC3	Theater and Tactical C3	Interoperability of C3 systems
IS	Information Systems	DoD transition to GOSIP
IS-IT	Information System—Information Technology	Corporate information management, DoD data standardization, functional process improvement
ASD(P&L)	Production and Logistics	Standards development
S&DS	Standardization & Data Management	Distribution of standards
DIA	Defense Intelligence Agency	
DISA (formerly DCA)	Defense Information Systems Agency	DoD Executive Agent for data comm protocol standards
DCS Organ	Defense Communications System Organization	
JIEO	Joint Tactical C3 Agency	Lead for tactical communication technical standards
JINTACCS	Joint Interoperability Tactical C2 Systems Program	Joint message standards
JMSWG	JTIDS Message System WG	TADIL J; J-Series messages and protocols
FSSG	Fire Support Subgroup	K-Series messages (and protocols)
DMTD	Digital Message Transfer Device Subgroup	MIL-STD-200-220
DTMP	DCPS Technical Management Panel	DoD data communications (including OSI) standards development
JITF	Joint Interface Test Force	Testing Joint interfaces
JITC	Joint Interoperability Test Center	Testing Joint interfaces
CIM	Corporate Information Management	Data standardization, data administration, functional process improvement
JDSSC	Joint Data Systems Support Center	
JSC	Joint Steering Committee	Develop common interoperability standards
DLA	Defense Logistics Agency	
DMSSO	Defense Materiel Specifications & Standards Office	—
NSA	National Security Agency	Security criteria and standards
JCS J-6J	Joint Tactical C3 Systems Division	Ensure interoperability of TDSs
MCEB	Military Communications-Electronics Board	Coordinate representation to international standards bodies
USA DISC4	Director, Information Systems for C4	Technical requirements, interoperability
SAIS-ADO	RSI-Rationalization, Standards, & Interoperability	Interoperability and standards
DCSOPS	International RSI	Operational requirements, interoperability
PEO CCS	PEO Command & Control Systems	Interoperability of Army Tactical C2 Systems
PEO Comm	PEO Communications	Interoperability of Communications Systems
AMC	Army Materiel Command	Materiel standards
ICP-M	Office of International Cooperative Programs	
CECOM	Communications & Electronics Command	
TRADOC	Training and Doctrine Command	Operational and procedural standards
CAC	Combined Arms Command	
SIGCEN	Signal Center	Communications standards
USAISC	Information Systems Command	
ISEC	Information Systems Engineering Command	

Table F-4. Responsibilities for Communications and Information Processing in U.S. Standards Bodies (Cont'd)

USN Info MGT	Information Management	
ASN	C3I and Space	
RE&S/C3I&Space		
CNO/SPAWAR	Space & Naval Warfare Systems Command	—
CNO/Space,C2	Space & C2	
OP-945	Information Management Support	
NAVDAC	Naval Data Automation Command	
USMC Systems SI Command	Systems Integration	Standards
MCCDC-WFC	Warfighting Center	Requirements
HQMC (C412) D4 Div P&I	Planning and Interoperability	Standards coordination
USAF AQ/DAS C4F	Acquisitions--C4	
ACS C4 Sys	C4 Systems	
AF Comm Cmd	Communications Command	
AFSC	Air Force Systems Command	—
ESD	Electronic Systems Division	
RADC	Rome Air Development Center	
ACC	Air Combat Command (air component of Atlantic Command)	

Table F-5. ANSI X3 Technical Committees[16]

X3A1	OCR and MICR	X3J16	C++
		X3J17	Prolog
X3B5	Digital Magnetic Tape	X3J18	REXX
X3B6	Instrumentation Tape	X3J19	Xbase
X3B7	Magnetic Disks	X3J20	Smalltalk
X3B9	Paper Forms/Layout		
X3B10	Identification Cards & Related Devices	X3K5	Vocabulary
X3B11	Optical Digital Data Disks		
		X3L1	Spatial Data Transfer
X3H2	Database	X3L2	Codes & Character Sets
X3H3	Computer Graphics	X3L3	Audio/Picture Coding
X3H4	Information Resource Dictionary System	X3L8	Data Representation
X3H5	Parallel Processing Constructs for High Level Programming Languages		
X3H6	Case Tool Integration Model	X3S3	Data Communications (lower layers)
X3H7	Object Information Management		
		X3T2	Data Interchange
X3J1	PL/1	X3T3	Open Distributed Processing
X3J2	BASIC	X3T4	Security Techniques
X3J3	FORTRAN	X3T5	Open Systems Interconnection (upper layers)
X3J4	COBOL	X3T6	Non-Contact Information Systems Interface
X3J7	APT	X3T7	Internationalization
X3J9	PASCAL	X3T8	Fault Isolation
X3J10	APL	X3T9	I/O Interface
X3J11	C		
X3J12	DIBOL	X3V1	Text: Office & Publishing Systems
X3J13	Common LISP		
X3J14	FORTH	X3W1	Office Machines
X3J15	DATABUS		

16 Updated from *X3 Projects Manual X3/SD-4*, July 1993 [Ref. ANSI 1993].

Under the AS method, an organization sponsors a drive for standardization and begins the canvass method by inviting comments on the proposed standard from anyone who cares or may be materially affected by it. This method is appropriate only when substantial agreement on the document to be standardized already exists, as was the case with the Ada programming language standard [Cargill 1989, 104].

In the AO method, an existing group completes a standard in an area in which it has direct and material interest and a perceived expertise. Usually an industry trade group or association of industry experts or participants, the AO often has extant standards that are based on the methodologies of its profession or discipline [Cargill 1989, 105]. The IEEE Computer Society is an example of an AO.

The ASC takes groups and factions with diverse, even antagonistic viewpoints and melds them into a semicohesive whole, with the aim of engineering a solution that encompasses all of the diversity while maintaining the benefits of individuality. The key to the ASC is the Secretariat, held by a sponsoring organization, which provides legal, administrative, and financial backing [Cargill 1989, 107]. The Computer and Business Equipment Manufacturers Association (CBEMA) is the Secretariat for ASC X3 on Information Processing Systems standards. In addition to developing, reviewing, and approving proposed American National Standards, the ASCs coordinate standardization activities on the international level by participating in the ISO.

The National Computer Systems Laboratory (NCSL) at the NIST contributes to the development of industry-wide standards by leading and participating in the work of organizations such as ANSI, IEEE, and ISO. In addition it develops tests and test methods for new standards. NIST prepares and the Department of Commerce issues Federal Information Processing Standards Publications (FIPS PUBS). Wherever possible, the FIPS are aligned with or identical to ANSI or ISO standards. However, when the government needs a standard, and the industry and its standards groups do not respond to this need, the NCSL has the ability to develop its own FIPS [Cargill 1989, 213].

The Department of Defense (DoD) also issues standards, called MIL-STDs or DoD-STDs, through its Quality Standardization Program. Where there is no substantial or demonstrable advantage to DoD in the development of a new standard, non-Government specifications and standards are to be adopted [DoD 1976, p.2]. The DISA is responsible for developing military standards in communications and information technology.

The Center for Information Management (CIM) Infrastructure office within DISA has the responsibility for defining requirements and priorities for standards development. The Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) [formerly the Protocol Standards Technical Panel (PSTP)] was formed under the direction of the PSSG to investigate technical matters and develop recommendations for standardization.

Now a part of DISA, the JIEO is the lead agency for tactical communications standards. The Center for Standards centralizes the standards activity of DISA. The Joint Message Standards Working Group (JMSWG) is responsible for Joint Interoperability Tactical Command and Control System (JINTACCS) message text formats (MTFs) and tactical data links. The Joint Technical Standards Steering Group (JTSSG) sets policy for and approves the products of the MIL-STD-187 and MIL-STD-188 series standards activities.

4.9 Standards Bodies in Non-NATO Nations

Finland is represented in ISO and IEC by the Suomen Standardisoimisliitto (SFS).

Sweden is represented in ISO by the Standardiseringskommisionen i Sverige (SIS). SIS coordinates with the Swedish Electrical Commission (SEK) and the Swedish Mechanical Standardization (SMS).

The Irish member of ISO and CEN is the National Standards Authority of Ireland (NSAI), an autonomous unit of the Institute for Industrial Research and Standards (IIRS).

The Japanese Industrial Standards Committee (JISC) oversees the Japanese Industrial Standards (JISs). The JISC is attached to the Agency of Industrial Science and Technology, Ministry of International Trade and Industry (MITI). JISC members include representatives from manufacturers, consumers, and knowledgeable individuals. Texts of standards approved by the relevant Minister and announced in the Government Gazette are published by the Japanese Standards Association (JSA). An Information Technology Standardization Technology Committee (INSTAC) within the Japanese Standards Association, the Telecommunications Technology Committee (TTC), the Interoperability Database System Development Project, and the Interoperability Association for Information Processing (INTAP) were established in 1985 to promote interoperability technology. INTAP has the responsibility to develop functional standards and conformance tests for OSI in Japan.

The Saudi Arabian Standards Organization (SASO) represents Saudi Arabia in ISO and IEC.

APPENDIX G

STATUS OF OPEN SYSTEMS STANDARDS DEVELOPMENT IN ISO/IEC

STATUS OF OPEN SYSTEMS STANDARDS DEVELOPMENT IN ISO/IEC[1]

1. INTRODUCTION

This appendix provides an overview of the work plans of selected technical committees and working groups in ISO/IEC as well as the work plan for ITU-TS SG7. The purpose is to illustrate how rapidly international civil standards are being progressed in those areas applicable to automated information systems. A compilation of ISO/IEC and ITU-TS standards is provided in Appendix D (by layer of the OSI Reference Model) and Appendix E (numerical listing). An overview of international standards bodies and their responsibilities for standards development is provided in Appendix F. The information in this Appendix is as of November 1993.

2. STANDARDIZATION QUESTIONS FOR SC21 WORKING GROUPS[2]

Working groups in SC21 address new standardization topics through a series of questions, some of which are closed by subsequent study and others lead to new work item proposals. Listed below are the open and recently closed questions. The digit following the letter "Q" indicates the working group that originated the question. Thus Q 1/17.2 is the seventeenth question (Subdivision 2) from SC21/WG1.

- WG1 Questions on OSI Architecture
  - Q 1/17.2 Maintenance of list of definitions collected in OSI standards and draft standards
  - Q 1/29 Upper layer architecture coordination (no current work)
  - Q 1/30 Lower layer architecture coordination (no current work)
  - Q 1/41 OSI management architecture coordination (no current work)
  - Q 1/48.6 LOTOS enhancements [SC21 N 7096, draft answer]
  - Q 1/49.8 Conformance and registration [SC21 N 8007, final answer]
  - Q 1/49.9 Long-term solution on general and dependent conformance [SC21 N 8008, final answer]
  - Q 1/53.1 Work on security in SC21 [SC21 N 3267, draft answer]
  - Q 1/54 Multipeer data transmission coordination
  - Q 1/63.2 Testability of managed objects [SC21 N 8009, draft answer]
  - Q 1/65.1 User requirements for OSI systems supporting time critical communications
  - Q 1/65.2 OSI protocol efficiency
  - Q 1/66 ODP conformance testing methodology
  - Q 1/67 Generalization of application service object (ASO) concepts
  - Q 1/68 Definition of the term "application process title" in the OSI Reference Model [SC21 N 7990, final answer]
  - Q 1/69 Conformance assessment for OSI security
  - Q 1/70 Clarification of the use of NIL selectors [SC21 N 8001, draft answer]
  - Q 1/71 Combined test purposes
- WG3 Questions on Database
  - Q 3/001 Support for objects in database [SC21 N 7180, draft answer]
  - Q 3/002 Test embedded in structured databases
  - Q 3/003 Interpretation of expression evaluation (question closed; incorporated in DIS 9075)
  - Q 3/004 Read-only cursors (question closed; incorporated in DIS 9075)
  - Q 3/005 Semantics of working view tables (question closed; incorporated in DIS 9075)
  - Q 3/006 Module authorization identifiers (question closed; incorporated in DIS 9075)
  - Q 3/007 Distributed database systems
  - Q 3/008 IRDS definition-level content standards for semantic unification meta model (SUMM) (question withdrawn June 1993)
  - Q 3/009 Approach to remote IRDS access [SC21 N 7181, draft answer]
  - Q 3/010 ODP and distributed database systems

---

1 This Appendix was updated from *ISO/IEC JTC1/SC21 Programme of Work*, November 1993 [SC21 SD-2].

2 Updated February 1994 based on [DRA 1994], January 1994, and *Status Report on ITU-TS Study Group Activities* [SC21 N 6956], June 1992.

- Q 3/011 Harmonization of client server capabilities
- Q 3/012 Basic object type taxonomies for IRDS
- WG4 Questions on OSI Management
  - Q 4/001 OSI Software management (question closed)
  - Q 4/002 Access to distributed Directory information by a single name [SC21 N 7935, draft answer]
  - Q 4/003 Directory APIs (failed registration ballot)
  - Q 4/004 Directory schema migration [SC21 N 7934, draft answer]
- WG7 Questions on Open Distributed Processing
  - Q 7/001 Use of Z in ODP [SC21 N 7051, draft answer]
- WG8 Questions on OSI Upper Layers
  - Q 8/001 Versions and extensibility [SC21 N 7909, draft answer]
  - Q 8/002 Relationship between ULA and ODP [SC21 N 7910, final answer].

Study questions of the ITU-TS SG7 on Data Networks and Open System Communications for the 1993-1996 study period are the following:

- Q 1/7, Standardization of the technical characteristics of international data transmission services, user classes of service, optional user facilities, and call progress signals in public data networks (PDNs) and ISDNs and the categories of access for DTEs to such services
- Q 2/7, Network Performance and Quality of Service in Data Communication Networks
- Q 3/7, Numbering Plan for Public Data Networks
- Q 4/7, Routing Principles for Public Data Networks
- Q 5/7, Multicast
- Q 6/7, Further study of interworking cases specific to public data networks
- Q 7/7, Further study of the DTE/DCE interfaces for packet-mode data terminal equipments
- Q 8/7, Study of DTE/DCE interface procedures for Dissimilar Terminal Interworking
- Q 9/7, Packet mode signalling between public networks providing data transmission service
- Q 10/7, Requirements, arrangements and interface characteristics for the provision of data services, in PSDNs when accessed via the ISDNs, and in ISDNs
- Q 11/7, Principles of management for public data networks and for the Customer Network Management Service
- Q 12/7, Management aspects of interworking between public data networks and between public data networks and other networks
- Q 13/7, Open Systems Interconnection (OSI) Systems Management
- Q 14/7, Message Handling Systems (MHS)
- Q 15/7, Directory Systems
- Q 16/7, Reference Model and Components for Open Distributed Processing
- Q 17/7, Testing of Data Communication Protocols
- Q 18/7, X.400/X.500 Conformance Testing
- Q 19/7, Open Systems Interconnection (OSI) Architecture
- Q 20/7, Security services, mechanisms and protocols for ITU-TS applications
- Q 21/7, Open Systems Interconnection (OSI) Application Layer
- Q 22/7, Open Systems Interconnection (OSI) Presentation and Session Layers
- Q 23/7, Open Systems Interconnection (OSI) Transport and Network Layers
- Q 24/7, Open Systems Interconnection (OSI) Data Link and Physical Layers
- Q 25/7, Revision of Recommendations.

3. INFORMATION PROCESSING STANDARDS (JTC1)

Tables G-1 to G-5 provide[3] an overview of the work plans for the major working groups of ISO/IEC JTC1/SC21, whose responsibility is Information Retrieval, Transfer, and Management for OSI. The standards bodies included in this table are:

- WG1 on OSI Architecture
- WG3 on Database

---

3 These tables are based on a format development by Technology Appraisals, Limited. The original versions of the tables were taken from "Standard Status--SC21 Information Retrieval, Transfer, and Management of OSI" [Ref. Payton 1988 (used with permission). The authors wish to acknowledge additional contributions from Alan Payton and Technology Appraisals, Limited, during the years 1989-1994.

- WG4 on OSI Management and OSI Directory
- WG7 on Open Distributed Processing[4]
- WG8 on OSI Upper Layers (formerly WG5 on Specific Application Services and Protocols and WG6 on Session, Presentation, Common Application Service Elements, and Upper Layer Architecture)
- WG 9 on Testing

The symbols used in Tables G-1 to G-5 show the progress of a standard from its submission as a working draft (circulated to SC21), through the intermediate stages of committee draft (CD) or draft proposal (DP) and draft international standard (DIS), in becoming an international standard. The position of each symbol indicates the approximate time of year the milestone represented by the symbol is expected to occur. No symbols are used for those standards that reached IS status in years prior to 1993.

Table G-1. Status of Standards Development in ISO/IEC JTC1 SC21/WG1

WG1 OSI ARCHITECTURE	CURRENT STANDARD	1993	1994	1995
OSI Reference Model	ISO 7498: 1984			
Pt 1: Basic Reference Model	ISO 7498-1: 1984			
Revision	SC21 N 8228			
Connectionless data transmission	ISO 7498 AD1			
Multipeer data transmission (MPDT)	ISO 7498 PDAD 2		PROJECT SUSPENDED	
Arch. for Multipeer Data Comm	SC 21 N 8003		New Work Item	
Pt 2: Security architecture	ISO 7498-2: 1989			
Pt 3: Naming and addressing	ISO 7498-3: 1989			
OSI Service Conventions	TR 8509: 1987			
Conventions for service definition	DIS 10731			
Tutorial on Naming and Addressing	TR 10730: 1993			
Amendment 1: Directory names	SC21 N 7998			
Concepts and Terminology for Conceptual Schema and Info Base	TR 9007: 1987			
Security Frameworks in Open Systems	DIS 10181			
Pt 1: Overview	CD 10181-1.2			
Pt 2: Authentication	DIS 10182-2.2			
Pt 3: Access control	DIS 10181-3			
Pt 4: Non-repudiation	CD 10181-4			
Pt 5: Confidentiality	CD 10181-5			
Pt 6: Integrity	CD 10181-6			
Pt 7: Security audit framework	CD 10181-7.2			
Quality of Service Framework	SC21 N 7993			
Formal Methods in Conformance Testing	SC21 N 7995			
Conformance Testing Methodology and Framework	ISO 9646			
Pt 1: General aspects	ISO 9646-1: 1991			
Revision 9646-1				
Protocol profile testing meth.	DAM 1			
Multiparty testing methodology	DAM 2			
Pt 2: Abstract test suite spec.	ISO 9646-2: 1991			
Revision 9646-2				
Protocol profile testing meth.	DAM 1			
Multiparty testing methodology	DAM 2			
Pt 3: TTCN	ISO 9646-3: 1992			
TTCN extensions	DAM 1			
Further extensions	PDAM 2			
Pt 4: Test realization	ISO 9646-4: 1991			
Revision 9646-4				
Protocol profile testing meth.	DAM 1			
Multiparty testing methodology	DAM 2			

4 The table for WG7 is short and is placed after the table for WG1.

Table G-1. Status of Standards Development in ISO/IEC JTC1 SC21/WG1 (Cont'd)

WG1 OSI ARCHITECTURE	CURRENT STANDARD	1993	1994	1995
Pt 5: Req. test labs and clients	ISO 9646-5: 1991			
Revision 9646-5			■	
Protocol profile testing meth.	DAM 1	■		
Multiparty testing methodology	DAM 2	■		
Pt 6: Protocol profile test spec.	DIS 9646-6	■		
Pt 7: Req. on ICS and guidance	DIS 9646-7		■	
Extensions to 9646 on Testing & OSI protocols over OSI services provided by non-OSI protocols	SC21 N 8016			
Open Systems Assessment. Methodology	SC21 N 8010			
Formal Description Techniques				
Estelle	ISO 9074:1989			
Estelle tutorial	AM 1			
Revision				■
LOTOS	ISO 8807: 1989			
G-LOTOS	DAM 1	■		
Guidelines for Application of Estelle, LOTOS and SDL	TR 10167: 1991			

Key: ☐ WD ⧄ DIS
⊡ DP/CD ■ ISO

Table G-2. Status of Standards Development in ISO/IEC JTC1 SC21/WG7

WG7 OPEN DISTRIBUTED PROCESSING	CURRENT STANDARD	1993	1994	1995
Open Distributed Processing (ODP)				
Pt 1: Overview and Guide to Use	WD 10746-1		⊡	⧄
Pt 2: Descriptive model	CD 10746-2.3		⧄	■
Pt 3: Prescriptive model	CD 10746-3.2		⧄	■
Pt 4: User guide (merged w/ Part 1)	old WD 10746-4			
Pt 4: Arch. semantics, formalisms	WD 10746-4		⊡	⧄
TR on use of specification tech. in ODP	SC21 N 7052		⊡	⧄
ODP Trader	SC21 N 8192		⊡	

Key: ☐ WD ⧄ DIS
⊡ DP/CD ■ ISO

Table G-3. Status of Standards Development in ISO/IEC JTC1 SC21/WG3

WG3 DATABASE	CURRENT STANDARD	1993	1994	1995
Database Languages	-			
NDL	ISO 8907: 1987			
SQL (with integrity enhancement)	ISO 9075: 1989			
SQL 2	ISO 9075:1992			
Call Level Interface	Part X	□	▣ ⧄	■
Persistent SQL Modules	Part Y	□	▣ ⧄	■
SQL 3	WD 9075.3		▣	
Export/Import for SQL			PROJECT TERMINATED	
Design Support for SQL Applications	SC21 N 5152	□	▣	⧄
SQL Multimedia (SQL/MM)				
Pt 1: Framework			□	▣
Pt 2: Facilities for SQL			□	▣
Pt 3: Facilities for IRDS			□	
Information Resource Dictionary System (IRDS)				
Framework	ISO 10027: 1990			
Revision of IRDS Framework	SC21 N 8204		▣	⧄
Services interface	ISO 10728: 1993			
C :Language Binding	PDAM 1		⧄	■
Ada Language Binding	WDAM 2		▣	⧄
Extensions	SC21 N 8202		▣	⧄
Export/Import for IRDS	SC21 N 5137		PROJECT TERMINATED	
Command language	DP 8800-1		PROJECT TERMINATED	
Guidelines for Design of IRDS Content Modules		□	▣	⧄
Reference Model of Data Management	ISO 10032			
Application of RM of data management	SC21 N 4119	□		▣
Data Management Export/Import Facilities				
Pt 1: Framework		□	▣	⧄
Pt 2: Facilities for SQL			□	▣
Pt 3: Facilities for IRDS		□	▣	⧄
Remote Database Access (RDA)	DIS 9579			
Pt 1: Generic model, service, & prot.	DIS 9579-1	■		
Generic RDA	WDAM 1		▣	⧄
Pt 2: SQL specialization	DIS 9579-2	■		
Pt 3: SQL PICS proforma	CD 9579-3	▣	⧄	■
Support for SQL 2	SC 21 N 7198		▣	⧄
RDA Tutorial (future technical report)	SC21 N 3343		PROJECT TERMINATED	
RDA Support for stored DBL statements			□	▣

Key: □ WD ⧄ DIS
▣ DP/CD ■ ISO

Table G-4. Status of Standards Development in ISO/IEC JTC1 SC21/WG4

WG4 OSI MANAGEMENT AND OSI DIRECTORY	CURRENT STANDARD	1993	1994	1995
OSI Reference Model--Management Framework	ISO 7498-4: 1989			
Systems Management Overview	ISO 10040: 1992			
Mgmt. knowledge management	DAM 1			
Mgmt. domains architecture	PDAM 2			
Gen & dependent conformance	PDAM 3			
Systems Management Tutorial	SC21 N 4942		PROJECT TERMINATED	
Systems Management (functions)	ISO 10164			
Pt 1: Object management function	ISO 10164-1: 1993			
ICS Proformas	DAM 1			
Pt 2: State management function	ISO 10164-2: 1993			
ICS Proformas	DAM 1			
Pt 2: Relationship attributes for representation	ISO 10164-3: 1993			
ICS Proformas	DAM 1			
Pt 4: Alarm reporting function	ISO 10164-4: 1992			
ICS Proformas	DAM 1			
Pt 5: Event report mgmt. function	ISO 10164-5: 1993			
ICS Proformas	DAM 1			
Enhanced discriminator	WDAM 2			
Pt 6: Log control function	ISO 10164-6: 1993			
ICS proformas	DAM 1			
Enhanced log	WDAM 2			
Pt 7: Security alarm reporting fctn.	ISO 10164-7: 1992			
ICS Proformas	DAM 1			
Pt 8: Security audit trail function	ISO 10164-8: 1993			
Pt 9: Objects & attributes for access control	DIS 10164-9			
Pt 10: Usage metering function	DIS 10164-10.2			
ICS Proforma	WDAM 1			
Pt 11: Metric objects and attributes	DIS 10164-11			
ICS Proforma	WDAM 1			
Add'l metric objects & attributes	WDAM 2			
Pt 12: Test management function	DIS 10164-12			
ICS Proforma	PDAM 1			
Pt 13: Summarization function	DIS 10164-13			
ICS Proforma	WDAM 1			
Additional summary scanners	WDAM 2			
Pt 14: Confidence & diagnostic test.	DIS 10164-14			
Pt 15: Scheduling function	DIS 10164-15			
Pt 16: Mgmt. knowledge mgmt fctn.	CD 10164-16.2			
Pt 17: Change over function	CD 10164-17			
Pt 19: Mgmt. domain & mgmt. policy mgmt. function	CD 10164-19			
Mngd. objects for supp. upper layers	WD 10164-mo			
Gen. relationship mgmt. function	WD 10164-rm.2			
Time management function	WD 10164-tm.2			
Software management	WD 10164-sw			
Response time monitoring	WD 10164-rtm			
Enhanced event control function	WD 10164-ev.2			
Ext. fnct. for systems mgmt. comm	SC21 N 7970			
Applic. context for SM with TP	CD 11587.2			

Table G-4. Status of Standards Development in ISO/IEC JTC1 SC21/WG4 (Cont'd)

WG4 OSI MANAGEMENT AND OSI DIRECTORY	CURRENT STANDARD	1993	1994	1995
Structure of Management Information	ISO 10165			
Pt 1: Management information model	ISO 10165-1: 1993			
Generalization of terms from GRM	PDAM 1			
Pt 2: Definition of mgmt. information	ISO 10165-2: 1992			
Enhanced discriminator and log	PDAM 1.2			
Pt 3: Mgmt info regis & regis proc.			PROJECT TERMINATED	
Pt 4: Guidelines for definition of managed objects	ISO 10165-4: 1992			
Set by create and component relationship	PDAM 1			
Pt 5: Generic mgmt. information	DIS 10165-5			
Pt 6: Guidelines for conformance mgmt. statement	DIS 10165-6			
Manager role conformance	WDAM 1			
Pt 7: General relationship model	CD 10165-7.2			
Command Sequencer for Systems Management	SC21 N 7962			
Common Management Information				
Service definition (CMIS)	ISO 9595: 1991			
Protocol specification (CMIP)	ISO 9596-1: 1991			
Support for allomorphism	PDAM 3		PROJECT TERMINATED	
Access control	AM 4: 1992			
PICS proforma	ISO 9596-2			
The Directory				
Pt 1: Overview	ISO 9594-1: 1990			
Replication, schema & access ctrl.	DAM 1			
Pt 2: Information framework	ISO 9594-2: 1990			
Access control	DAM 1			
Schema extensions	DAM 2			
Replication	DAM 3			
Pt 3: Abstract service definition	ISO 9594-3: 1990			
Access control	DAM 1			
Replication, schema, and enhanced search	DAM 2			
Pt 4: Procedures for dist. operations	ISO 9594-4:1990			
Access control	DAM 1			
Replication, schema, and enhanced search	DAM 2			
Pt 5: Protocol specification	ISO 9594-5:1990			
Replication	DAM 1			
Pt 6: Selected attribute types	ISO 9594-6: 1990			
Schema extensions	DAM 1			
Pt 7: Selected object classes	ISO 9594-7: 1990			
Schema	DAM 1			
Pt 8: Authentication framework	ISO 9594-8: 1990			
Access control	DAM 1			
Extension to 9594-8 on security	WDAM			
Pt 9: Replication & knowledge mgmt.	ISO 9594-9:1993			

Table G-4. Status of Standards Development in ISO/IEC JTC1 SC21/WG4 (Cont'd)

WG4 OSI MANAGEMENT AND OSI DIRECTORY	CURRENT STANDARD	1993	1994	1995
Pt 10: DUA PICS Proforma	WD 9594-10	⧄	■	
Pt 11: DSA PICS Proforma	WD 9594-11	⧄	■	
Use of systems mgmt. for administration of dir.	SC21 N 7930 WD 9594-?		▣	⧄
Internationalization of dir.	SC21 N 7931	□	▣	⧄
Enhan. of Directory oper. security	SC21 N 7932	□	▣	⧄
Overview - to track 1993 Directory incorporating approved amendments AM) and technical corrigenda (TC) from ITU-TS		■		
Info. Framework - to track 1993 Directory incorporating approved AM & TC		■		
Abstract Service Def - to track 1993 Directory incorporating approved AM & TC		■		
Distributed Ops - to track 1993 Directory incorporating approved AM & TC		■		
Protocol Spec - to track 1993 Directory incorporating approved AM & TC		■		
Selected Attribute Types - to track 1993 Directory incorporating approved AM & TC		■		
Selected Object classes to track 1993 Directory incorporating approved AM & TC		■		
Authentication Frame to track 1993 Directory incorporating approved AM & TC		■		

Key: □ WD ⧄ DIS
▣ DP/CD ■ ISO

Table G-5. Status of Standards Development in ISO/IEC JTC1 SC21/WG8

WG8 OSI UPPER LAYER	CURRENT STANDARD	1993	1994	1995
Application Layer Structure (ALS)	ISO 9545: 1993			
Extended ALS (XALS)	ISO 9545: 1993			
Modeling recovery in application layer	WDAM 2	PROJECT TERMINATED		
Amendment covering CL mode op.		PROJECT TERMINATED		
Revision of 9545	DIS 9545			
Association Control Service Element (ACSE)				
Revision 8649				
Service definition	ISO 8649: 1988			
Authentication	AM 1			
Appl. Context Neg.	DAM 3			
Protocol specification	ISO 8650:1988			
Revision 8650				
Authentication	AM 1:1990			
A-context specification	DAM 2			
PICS proforma	DIS 8650-2			
Extensions to ACSE on ASOs and ASO Associations				
Commitment, Concurrency, and Recovery (CCR)				
Service definition	ISO 9804: 1990			
Revision of 9804				
Enhancements	PDAM 1			
Session mapping changes	AM 2:1990			
Protocol specification	ISO 9805: 1990			
Revision of 9805				
Enhancements	PDAM 1			
Session mapping changes	AM 2:1990			
PICS proforma	DIS 9805-2			
LOTOS description of CCR service	PDTR 11589			
LOTOS description of CCR protocol	PDTR 11590			
Conformance Test Suite for the CCR Protocol				
Reliable Transfer (RTSE)				
Pt 1: Model and Service	ISO 9066-1: 1989			
Pt 2: Protocol	ISO 9066-2: 1989			
Pt 3: PICS Proforma	CD 9066-3			
Remote Operations (ROSE)				
Pt 1: Model, notation & service def.	ISO 9072-1: 1989			
Support of built-in operations	PDAM 1			
Revision	DIS 9072-1			
Pt 2: Service definition	ISO 9072-2: 1989			
Revision	DIS 9072-2			
Support of built-in operations	PDAM 1			
Pt 3: Protocol specification	DIS 9072-3			
Support of built-in operations	PDAM 1			
Pt 4: PICS Proforma	CD 9072-4			
Enhancements to Pts 1-3	SC21 6718-6719	PROJECT TERMINATED		
Generic Upper Layer Security (GULS)				
Pt 1: Overview, model, and notation	DIS 11586-1			
Pt 2: SESE definition	DIS 11586-2			
Pt 3: Protocol specification	DIS 11586-3			
Pt 4: Protecting transfer syntax	DIS 11586-4			
Pt 5: PICS Proforma	WD 11586-5			
Pt 6: Protecting transfer PICS	WD 11586-6			
Representation of Numerical Values in Character Strings	ISO 6093: 1985	Standard reaffirmed at SC21 Aries meeting, June 1991		

Table G-5. Status of Standards Development in ISO/IEC JTC1 SC21/WG8 (Cont'd)

WG8 OSI UPPER LAYER	CURRENT STANDARD	1993	1994	1995
Remote Procedure Call (RPC)				
Pt 1: Model	DIS 11578-1			
Pt 2: Interface def. notation (IDN)	DIS 11578-2			
Pt 3: Service	DIS 11578-3			
Pt 4: Protocol	DIS 11578-4			
Pt 51: PICS Proforma	WD 11578-5	UNDER REASSESSMENT		
Procedures for Specific OSI Registration Authorities				
Pt 1: General procedures	ISO 9834-1: 1993			
Incorporation of object iden. comp.	WDAM 1			
Incorporation of def. of root arcs	WDAM 2			
Pt 2: Document types	ISO 9834-2: 1993			
Pt 3: Joint object identifiers	ISO 9834-3: 1990			
Alignment with 9834-1	WDAM 1			
Pt 4: VTE Profiles	ISO 9834-4: 1991			
Pt 5: VT Control Objects	ISO 9834-5: 1991			
Pt 6: Application titles	ISO 9834-6: 1993			
Virtual Terminal (VT)				
Basic class VT service	ISO 9040: 1990			
Additional functional units	AM 2:1993			
Basic class VT protocol	ISO 9041-1: 1990			
Additional functional units	AM 2:1992			
PICS proforma	DIS 9041-2			
File Transfer, Access and Mgmt (FTAM)				
Pt 1: General description	ISO 8571-1: 1988			
Revision of 8571-1				
Pt 2: Virtual filestore	ISO 8571-2: 1988			
Revision of 8571-2				
Pt 3: File service definition	ISO 8571-3: 1988			
Revision of 8571-3				
Pt 4: File protocol specification	ISO 8571-4: 1988			
Revision of 8571-4				
Pt 5: PICS Proforma	ISO 8571-5: 1990			
Filestore management	PDAM1			
Service enhancement	WDAM3	(To be progressed as a technical corrigendum)		
Revision of 8571-5				
Filestore management	AM 1:1992, Pts. 1-4			
Overlapped access	AM 2:1993, Pts. 1-4	(Amendment to Pt. 5 is under reassesment)		
Service enhancements	AM 3:1993, Pts. 1-4			
Security enhancements	WDAM 4, Pt. 1	(Amendments to Pts. 2,3, 5 suspended)		
Distrib. Transaction Processing (TP)				
Pt 1: Model	ISO 10026-1: 1992			
Pt 2: Service	ISO 10026-2: 1992			
Pt 3: Protocol	ISO 10026-3: 1992			
Security (AMs)	SC21 N 6232			
Associationn. pool mgmt. (AMs)	SC21 N 7604			
Commitment optimization (AMs)	SC21 N 8219, 8220			
Dialogue recovery & user suspension of dialogue	SC21 N 6710			
Subtransactions	SC21 N 6236			
Separation of TP data/commit. flows	SC21 N 6240			
PICS proforma	DIS 10026-4			
Application context proforma	DIS 10026-5			
Unstructured data transfer	DIS 10026-6			
Message queuing	CD 10026-7			
Heuristic decisions (amendments)		PROJECT TERMINATED		

Table G-5. Status of Standards Development in ISO/IEC JTC1 SC21/WG8 (Cont'd)

WG8 OSI UPPER LAYER	CURRENT STANDARD	1993	1994	1995
Job Transfer and Manipulation (JTM)				
Concepts and services	ISO 8831: 1992			
Basic class protocol	ISO 8832-1: 1992			
Terminal Management (TM)			PROJECT TERMINATED	
Model	CD 10184-1		PROJECT TERMINATED	
Service	WD 10184-2		PROJECT TERMINATED	
Protocol	WD 10184-3		PROJECT TERMINATED	
Conformance Test Suites for FTAM				
Test suite structure and purposes	ISO 10170-1: 1993			
Abstract test suite (ATS)	WD 10170-2		□ ⊡	◪
ACSE ATS embedded under FTAM	WD 10170-3		□ ⊡	◪
Presentation ATS embedded under FTAM	WD 10170-4		□ ⊡	◪
Session ATS embedded under FTAM	WD 10170-5		□ ⊡	◪
Conformance Test Suites for Basic Class VT Protocol				
Test suite structure and test purposes	DIS 10739-1			
Data Descriptive File for Information Exchange	ISO 8211: 1985			
Revision	DIS 8211		■	
Methodology Guidelines for Developing AL stds.	SC21 N 7902		⊡	◪
Upper Layer Security Model	DIS 10745	■		
Session Layer Services and Protocols				
Basic session service definition	ISO 8326: 1987			
Revision of 8326	SC21 N 8207		■	
Symmetric synchronization	AM 1			
Unlimited user data	AM 2			
Connectionless mode session	AM 3			
Additional resynchronization	AM 4:1992			
Remove Serial No. Lim.	WDAM 5		⊡	◪
Basic session protocol specification	ISO 8327: 1987			
Revision of 8327	SC21 N 8208		■	
Symmetric synchronization	AM 1			
Unlimited user data	AM 2			
Additional resynchronization	AM 3:1992			
Remove Serial No. Lim	WDAM 4		⊡	◪
Session PICS proforma	DIS 8327-2	■		
LOTOS desc. of session service	TR 9571: 1989		PROJECT TERMINATED	
LOTOS desc. of session protocol	TR 9572: 1989		PROJECT TERMINATED	
Pres. Layer Services and Protocols				
Basic CO presentation service def.	ISO 8822: 1988			
Revision of 8822	DIS 8822.2		■	
CL mode presentation service	AM 1:1991			
Unlimited user data	AM 2:1993	■		
Procedures for registration	DAM 3		■	
Symmetric synchronization	AM 4:1993	■		
Add'l session synchronization	AM 5:1992			
Basic CO pres. protocol spec.	ISO 8823: 1988			
Revision of 8823	DIS 8823-1		■	
Unlimited user data	DAM 2		■	
Syntax registration	DAM 3		■	
Symmetric synchronization	DAM 4		■	
Additional resynchronization functionality	AM 5:1992			
Confidentiality and integrity	WDAM 6	■		
Presentation PICS proforma	DIS 8823-2	■		

Table G-5. Status of Standards Development in ISO/IEC JTC1 SC21/WG8 (Cont'd)

WG8 OSI UPPER LAYER	CURRENT STANDARD	1993	1994	1995
Specification of ASN.1	ISO 8824: 1990			
Revision of 8824				
Basic ASN.1	DIS 8824-1			
Rules for extensibility	PDAM 3			
Removal of definition of root arcs	WDAM 4			
Information object classes	DIS 8824-2			
Constraint specification	DIS 8824-3			
Parameterization	DIS 8824-4			
Specification of Basic Encoding Rules for ASN.1	ISO 8825: 1990			
Revision of 8825				
Basic encoding rules	DIS 8825-1			
Packed encoding rules	CD 8825-2.2			
Disting. & canonical encoding rules	DIS 8825-3	(To be merged in text of DIS 8825-1)		
Lightweight encoding rules				
Authentication and Related Security Services for Distributed Operations	SC21 N 7914			
Connectionless Services and Protocols				
Session CL prot. to provide CL mode	ISO 9548			
PICS proforma for CL session prot.	DIS 9548-2			
CL pres. protocol to provide CL mode	ISO 9576: 1991			
PICS proforma for CL pres. protocol	DIS 9576-2			
CL ACSE service	ISO 8649 AM2:1990			
CL ACSE prot. to provide CL mode	ISO 10035: 1991			
PICS proforma for A-unit-data prot.	DIS 10035-2			
CL-mode operation for ALS				
Conform. Test Suite for Session Prot.				
Test suite struct. & test purposes	DIS 10168-1			
Generic test suite	WD 10168-2	PROJECT TERMINATED		
Abstract test suite for CS method	CD 10168-3			
Test mgmt. protocol specification	DIS 10168-4			
Conform. Test Suite for Pres. Layer	.			
Test suite struct. & test purposes	ISO 10729-1: 1993			
Test suite for ASN.1 encodings	DIS 10729-2			
Common pres. abstract test suite	WD 10729-3			
Conform. Test Suite for ACSE Protocol				
Test suite struct. & test purposes	ISO 10169-1: 1991			
Common ACSE abstract test suite	WD 10169-2			
Conform. Test Suite for CCR Protocol				
Conform. Test Suite for TP Protocol				
Pt. 1: TSS & TP	SC21 N 8216			
Pt. 2: Abstract Test Suite				
Test Management Protocol Spec.				
Interpretation of Accreditation Req's as specified in ISO/IEC Guide 25				

Key: WD DIS DP/CD ISO

APPENDIX H

INTERNATIONAL MILITARY AND OTHER STANDARDS BASED ON OSI STANDARDS OR USED IN OPEN SYSTEMS PROFILES

I. NATO Standards
II. National Military Standards
III. Agreements from Regional Workshops
IV. National Standards and Papers

INTERNATIONAL MILITARY AND OTHER STANDARDS BASED ON OSI STANDARDS OR USED IN OPEN SYSTEMS PROFILES

I. NATO STANDARDS

A. OSI STANAGs[1]

STANAG 4250◆[2]	NATO Reference Model for OSI, Edition 2, MAS/212-EL/4250, Military Agency for Standardization, 21 August 1990 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 7498)
STANAG 4250-1◆	NATO Reference Model for OSI, Part 1--General Description, Edition 2 of STANAG 4250, MAS/212-EL/4250, TSGCE SG9, 21 August 1990 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 7498-1)
STANAG 4250-1.3	NATO Reference Model for Open Systems Interconnection, Part 1--Basic Reference Model, Edition 3 of STANAG 4250, Draft, DS(CCC-ICP)(93)703 (distributed for staffing), SG9/WG6, 11 November 1993, NATO UNCLASSIFIED (work to include ISDN Reference Model in STANAG 4250 and retitle Part 1 as NATO Reference Model for Open Systems Information Exchange was suspended since agreement was not reached in TSGCE SG9 in October 1993)
STANAG 4250-2◆	NATO Reference Model for OSI, Part 2--Security, Draft, Version 4.0, December 1993 (submitted for staffing, final editing, and translation prior to distribution for ratification), NATO SECRET (cf. ISO 7498-2)
STANAG 4250-3◆	NATO Reference Model for OSI, Part 3--Naming and Addressing, Draft, DS(CCC-ICP)(93)117 (distributed for staffing) and AC/302-D/647 (distributed for ratification), 12 March 1993, NATO UNCLASSIFIED (cf. ISO 7498-3) (as of 25 January 1994, ratified by four nations)
STANAG 4250-4◆	NATO Reference Model for OSI, Part 4--Management, Draft, DS(CCC-ICP)(93)1129 (distributed for staffing) and AC/302-D/648 (distributed for ratification), 26 April 1993, NATO UNCLASSIFIED (cf. ISO 7498-4, 10040) (as of 25 January 1994, ratified by four nations)
STANAG 4250-5X◆	NATO Reference Model for OSI, Part 5X--Military Factors, Draft (preliminary), 1992, NATO UNCLASSIFIED (submitted as Part 5; cancelled May 1993)
STANAG 4250-5Y	NATO Reference Model for OSI, Part 5Y—NATO-Adopted Civil Standards, Draft (preliminary), October 1993, NATO UNCLASSIFIED (submitted as Part 5; work suspended by action of TSGCE SG9 in October 1993)
STANAG 4250-6X	NATO Reference Model for OSI, Part 6X--NSP Guidelines, Draft (preliminary), 1992, NATO UNCLASSIFIED [submitted as Part 6; rejected by TSGCE SG9 plenary in December 1992 and cancelled in May 1993; when this document becomes stable (sometime in 1994), it will be subsumed into the *NOSIP Strategy*]
STANAG 4251◆	NATO Reference Model for OSI - Layer 1 (Physical Layer) Service Definition, Draft, DS(CCC-ICP)(93)123 (distributed for staffing, 17 March 1993) and AC/302-D/649 (distributed for ratification), 30 April 1993, NATO UNCLASSIFIED (cf. ISO 10731, 10022)
STANAG 4252◆	NATO Reference Model for OSI - Layer 2 (Data Link Layer) Service Definition, Draft, DS(CCC-ICP)(93)130 (distributed for staffing, 18 March 1993) and AC/302-D-651 (distributed for ratification), 26 March 1993, NATO UNCLASSIFIED (cf. ISO 10731, 8886-3)
STANAG 4253◆	NATO Reference Model for OSI - Layer 3 (Network Layer) Service Definition, Draft, DS(CCC-ICP)(93)166 (distributed for staffing; awaiting electronic copy and copies of referenced ISO standards before final translation can be completed), 18 March 1993, NATO UNCLASSIFIED (Appendix B is NATO CONFIDENTIAL) (cf. ISO 10731, 8348/AD2)
STANAG 4254◆	NATO Reference Model for OSI - Layer 4 (Transport Layer) Service Definition, Draft, DS(CCC-ICP)(93)168 (distributed for staffing; awaiting copies of referenced ISO standards before final translation can be completed), 19 March 1993, NATO UNCLASSIFIED (cf. ISO 10731, 8072)
STANAG 4255◆	NATO Reference Model for OSI - Layer 5 (Session Layer) Service Definition, MAS/04-EL/4255, Military Agency for Standardization, 22 January 1993 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 10731, 8326)
STANAG 4256◆	NATO Reference Model for OSI - Layer 6 (Presentation Layer) Service Definition, MAS/04-EL/4256, Military Agency for Standardization, 22 January 1993 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 10731, 8822, 8823)
STANAG 4257◆	NATO Reference Model for OSI - Layer 7 (Application Layer) Service Definition, Draft, DS(CCC-ICP)(93)174 (distributed for staffing, 19 March 1993) and AC/302-D/657 (dist ibuted for

1 Status from NATO International Military Staff as provided in *5-6 May 1993 Subgroup 9 Coordination Meeting*, JIEO/TBBD, 13 May 1993 and [Rannestad 1994b], 25 January 1994.

2 The symbol ◆ identifies standards listed in the base standards of the 1993 *NOSIP Strategy*.

ratification), 11 November 1993, NATO UNCLASSIFIED (cf. ISO 10731, 8649, 8649/AM1, 9066-1, 9072-1)

STANAG 4258• Specification of ASN.1, MAS/04-EL/4258, Military Agency for Standardization, 22 January 1993 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 8824)

STANAG 4259• Specification of Basic Encoding Rules for ASN.1, MAS/04-EL/4259, Military Agency for Standardization, 21 January 1993 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 8825)

STANAG 4261• NATO Reference Model for OSI - Layer 1 (Physical Layer) Protocol Specification, Draft, DS(CCC-ICP)(93)129 (distributed for staffing; awaiting copies of referenced ISO standards before final translation can be completed), 17 March 1993, NATO UNCLASSIFIED

STANAG 4262• NATO Reference Model for OSI - Layer 2 (Data Link Layer) Protocol Specification, Draft, DS(CCC-ICP)(93)128 (distributed for staffing, 18 March 1993) and AC/302-D/652 (distributed for ratification), 26 March 1993, NATO UNCLASSIFIED (cf. ISO 7776, 8802-2, 8802-3, 8802-5)

STANAG 4263• NATO Reference Model for OSI - Layer 3 (Network Layer) Protocol Specification, Draft, DS(CCC-ICP)(93)167 (distributed for staffing; awaiting electronic copy copies of referenced ISO standards before final translation can be completed), 19 March 1993, NATO UNCLASSIFIED (cf. ISO 8208, 8473, 8648, 8878, 8880-1, 8880-2, 8880-3, 8880-4, 9542, 11577, X.25)

STANAG 4264• NATO Reference Model for OSI - Layer 4 (Transport Layer) Protocol Specification, Draft, DS(CCC-ICP)(93)172 (distributed for staffing; awaiting electronic copy copies of referenced ISO standards before final translation can be completed), 19 March 1993 , NATO UNCLASSIFIED (cf. ISO 8073, 8073/AD2, 8073/DAM3, 8602)

STANAG 4265• NATO Reference Model for OSI - Layer 5 (Session Layer) Protocol Specification, MAS/04-EL/4265, Military Agency for Standardization, 22 January 1993 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 8327, 8327-2)

STANAG 4266• NATO Reference Model for OSI - Layer 6 (Presentation Layer) Protocol Specification, MAS/04-EL/4266, Military Agency for Standardization, 22 January 1993 (ratified and promulgated), NATO UNCLASSIFIED (cf. ISO 8822, 8823)

STANAG 4267• NATO Reference Model for OSI - Layer 7 (Application Layer) Protocol Specification, Draft, DS(CCC-ICP)(93)175 (distributed for staffing, 22 March 1993) and AC/302-D/658 (distributed for ratification), 25 November 1993, NATO UNCLASSIFIED (cf. ISO 8650, 8650/AM1, 9066-2, 9072-2))

STANAG 4406• NATO Reference Model for OSI - Military Message Handling System, Draft (in final editing), DS(CCC-ICP)(93)161 (distributed for staffing, 17 March 1993) and AC/302(SG/9)WP/33, 26 November 1993, NATO UNCLASSIFIED (cf. ISO 10021, 10611) (a revised draft that includes Annex D is planned for SG9 staffing in October 1994)

Main Body, Draft

Annex A—MMHS Extensions to ISO 10021 Series, Draft

Annex B—Security Aspects of MMHS (under development)

Annex C—Alpha Profile Set (a delta specification to EWOS profiles): AMH1x(M) on Common Facilities and AMH9x(M) on Military Messaging, Draft

Annex D—Alpha/ACP 127 Gateway (under development)

Annex E—Alpha/MMHS(84) Gateway (under development)

Annex F—Alpha/MHS(88) Gateway (under development)

Annex G—Beta Profile Set (under development)

Annex H—Beta/ACP 127 Gateway (under development)

Annex I—Beta/Alpha Gateway (under development)

STANAG 4407• NATO Reference Model for OSI - Systems Management, Draft, DS(CCC-ICP)(93)158 (distributed for staffing; awaiting copies of referenced ISO standards before final translation can be completed), 15 May 1993, NATO UNCLASSIFIED (cf. ISO 10165-1, 10165-2, 10165-4, 10164, 11183, 12059, 12060)

Main Body, Preliminary Draft

Annex A—Security of Management (under development)

Annex B—Military Features, Preliminary Draft

Annex C—The Development of NSPs for Systems Management, Preliminary Draft

Annex D—NSP zzzz: Basic Systems Management , Preliminary Draft (STANAG 4407-1)

STANAG 4408• NATO Standardized Profile TAdnnn(M) - Connection-mode Transport Service over Connectionless-mode Network Service, Draft, October 1993, NATO UNCLASSIFIED (to be distributed to the nations; following agreement and receipt of copies of referenced ISO standards, final editing and translation precedes distribution for ratification)

Part 1: Subnetwork Type Independent Requirements for Group TA, Draft (cf. ISO 10608-1)

Part 2: TA5n(M) Subnetwork Type Independent Requirements for LANs, Draft (cf. ISO 10608-2)

Part 3: TA51(M) Profile - CSMA/CD LAN Requirements, Draft (cf. ISO 10608-2)

Part 4: TA54(M) Profile - Fiber Distributed Data Interface (FDDI) LAN (Military) Requirements, Draft (cf. ISO 10608-6)

STANAG 4409• NATO Standardized Profile - Connection-mode Transport Service over Connection-mode Network Service (Military), Draft, DS(CCC-ICP)(93)231 (distributed for staffing; awaiting copies of

	referenced ISO standards before final translation can be completed), 7 April 1993, NATO UNCLASSIFIED
	Part 1: Definition of Profiles TC1111(M)/TC1121(M), Draft (cf. ISO 10609-6)
	Part 2: Subnetwork-Type Independent Requirements for Group TC, Draft (cf. ISO 10609-2)
	Part 3: Subnetwork Type Dependent Requirements for Permanent Access to a Packet Switched Data Network Using Virtual Call, Draft (cf. ISO 10609-9)
STANAG 4410◆	NATO Standardized Profile - Connectionless-mode Transport Service over Connectionless-mode Network Service, Draft, DS(CCC-ICP)(93)232 (distributed for staffing; awaiting electronic copy copies of referenced ISO standards before final translation can be completed), 7 April 1993, NATO UNCLASSIFIED
	Part 1: Subnetwork-Type Independent Requirements for Group UA, Preliminary Draft
STANAG 4413◆	NATO Standardized Profile - Relaying the Connectionless-mode Network Service
	Part 1: Subnetwork-Type Independent Requirements for Group RA, Edition 2, January 1993 (cf. ISO 10613-1) (under development)
	Part 2: Subnetwork-Type Dependent, Media Independent Requirements for LANs, Edition 2, January 1993 (cf. ISO 10613-2) (under development)
	Part 3: ISDN Subnetwork-Dependent, Media-Dependent Requirements for Circuit-Switched B-Channel Operation, Edition 2, January 1993 (under development)
	Part 4: Profile RA51.4212, Edition 2, January 1993 (under development)
STANAG 4459◆	ISDN Bearer Services, Draft (in final approval prior to submission for translation and ratification), DS(CCC-ICP)(93)233 (distributed for staffing, 7 April 1993) and AC/302-D/659 (distributed for ratification), 9 June 1993, NATO UNCLASSIFIED (cf. I.230)
STANAG 4460◆	Layer 1 Specifications for ISDN Basic Rate Access at the S/T Reference Point, Draft (in final approval prior to submission for translation and ratification), DS(CCC-ICP)(93)234 (distributed for staffing, 8 April 1993) and AC/302-D/660 (distributed for ratification), 9 June 1993, NATO UNCLASSIFIED (a second version is under development)
STANAG 4461◆	Layer 1 Specifications for ISDN Primary Rate Access at the S/T Reference Point, Draft (in final approval prior to submission for translation and ratification), DS(CCC-ICP)(93)235 (distributed for staffing, 8 April 1993) and AC/302-D/661 (distributed for ratification), 9 June 1993, NATO UNCLASSIFIED (a second version is under development)
STANAG 4462◆	Layer 2 Specifications for ISDN Basic and Primary Rate Access at the S/T Reference Point, Draft (in final approval prior to submission for translation and ratification), DS(CCC-ICP)(93)236 (distributed for staffing, 8 April 1993) and AC/302-D/662 (distributed for ratification), 9 June 1993, NATO UNCLASSIFIED (a second version is under development)
STANAG 4463◆	Layer 3 User to Network Call Control, Draft, DS(CCC-ICP)(93)237 (distributed for staffing), 8 April 1993, NATO UNCLASSIFIED (to be distributed for ratification as soon as the translation is completed; a second version is under development)
STANAG 4464◆	Signalling System No. 7 Message Transfer Part (MTP), Draft (to be distributed to the nations; following agreement, final editing, and translation, to be distributed for ratification)
STANAG 4465◆	Signalling System No. 7 ISDN User Part (ISUP) (under development)
STANAG 4466◆	ISDN Teleservices (under development)
STANAG 4467◆	ISDN Supplementary Services (under development)
STANAG 4468◆	QSIG (under development)

B. OTHER STANAGs AND AGREEMENTS[3]

AAP-3	Procedures for the Development, Preparation, Production and the Updating of NATO Standardization Agreeements (STANAGs) and Allied Publications (APs)
AAP-4	NATO Standardization Agreeements and Allied Publications
AAP-7	Allied Maritime Structures Messages, Military Agency for Standardizaton (see STANAGs 1020-1370)
AAP-6(Q)	NATO Glossary of Terms and Definitions for Military Use, Revision Q
AAP-15(D)	Glossary of Abbreviations Use in NATO Documents, Revision D, September 1990
ACP 121	Communications Instructions - General
ACP 123	Communications Instructions - Common Messaging Strategy and Procedures, Draft, February 1993
ACP 126	Communication Instructions - Teletypewriter/Teleprinter Procedures
ACP 127	Communication Instructions - Tape Relay Procedures
ACP-167(F)	Glossary of COmmunications-Electronics Terms, Revision F
ADatP-2(D)	NATO Glossary of Automatic Data Processing (ADP) Terms and Definitions, Revision D
ADatP-3	NATO Message Text Formatting System (FORMETS), ADSIA WG5 (see STANAGs 5500, 5620, and 5621; and ACP 127)
ADatP-11	Standard Operating Procedures for NATO Link 11, ADISA WG1

3 Revised bassed on [NIPD 1993, Volume VI] and [NATO 1993].

ADatP-12	Standard Operating Procedures for he Ship/Shore/Ship Buffer, ADISA WG4
ADatP-14	Standard Operating Procedures for NATO Link 14, ADISA WG1
ADatP-16	Standard Operating Procedures for NATO Link 16, ADISA WG4
AAP-20	Phased Armaments Programming System (PAPS)
ADatP-31	Standard Operating Procedures for NATO Link 1, ADISA WG4
IJMS D/4	Interim Joint Tactical Information Distribution System (JTIDS) Message Specifications, ADSIA WG5
IJMS D/5	IJMS Implementation Document
IJMS D/6	Standard Operating Procedures for IJMS, ADSIA WG4
STANAG 4146	Interim Specifications for Input/Output Interfaces in NATO Naval Data Handling Equipment
STANAG 4153	Standard Specification for an Asynchronous Serial Data Interface for Point to Point Connections and for Connection to Data Networks in NATO Naval Systems
STANAG 4156	Standard Specification for a Serial Data Interface for Synchronous Connections to a Data Network
STANAG 4159	NATGO Materiel Configuration Management Policy
STANAG 4175	Technical Characteristics of the Multi-Functional Information Distribution System (MIDS), TSGCE SG9 (complementary to STANAG 5516)
STANAG 4197	Modulation and Coding Characteristics that must be Common to Assure Interoperability of 2400 BPS Linear Predictive Encoded Digital Speech Transmitted Over HF Radio Facilities
STANAG 4198	Parameters and Coding Characteristics That Must Be Common to Assure Interoperability of 2400 BPS Linear Predictive Encoded Digital Speech
STANAG 4199	Uniform System of Exchange of Materiel Management Data
STANAG 4202	Transmission Envelope Characteristics for High Reliability Data Exchange between Land Tactical Data Processing Equipment Over Single Channel Radio Links
STANAG 4203	Technical Standards for Single Channel HF Radio Equipment
STANAG 4204	Technical Standards for Single Channel VHF Radio Equipment
STANAG 4205	Technical Standards for Single Channel UHF Radio Equipment
STANAG 4206	The NATO Multichannel Tactical Digital Gateway-System Standards
STANAG 4207	The NATO Multi-Channel Tactical Digital Gateway - Multiplex Group Framing Standards
STANAG 4208	The NATO Multi-Channel Tactical Digital Gateway - Signalling Standards
STANAG 4209	The NATO Multi-Channel Tactical Digital Gateway - Standards for Analogue to Digital Conversion of Speech Signals
STANAG 4210	The NATO Multi-Channel Tactical Digital Gateway - Cable Link Standards
STANAG 4211	The NATO Multi-Channel Tactical Digital Gateway - System Control Standards
STANAG 4212	The NATO Multi-Channel Tactical Digital Gateway - Radio Relay Link Standards
STANAG 4213	The NATO Multi-Channel Tactical Digital Gateway - Data Transmission Standards
STANAG 4214	International Routing and Directory for Tactical Communication Systems
STANAG 4231	Digital Interoperability Between UHF Tactical Satellite Communications Terminals
STANAG 4232	Digital Interoperability Between SHF Tactical Satellite Communications Terminals
STANAG 4233	Digital Interoperability Between EHF Tactical Satellite Communications Terminals
STANAG 4234	Radio Frequency Environmental Conditions Affecting the Design of Materiel for Use by NATO Forces
STANAG 4245	Secure and ECM Resistant HF Low Speed Digital Data Communications System
STANAG 4246	Have Quick and UHF Secure Jam Resistant Communications Equipment
STANAG 4249	NATO Multi-Channel Tactical Digital Gateway - Data Transmission Standards (Packet Switching Service)
STANAG 4250	The NATO Reference Model for Open Systems Interconnection - Overview
STANAG 4261	The NATO Reference Model for Open Systems Interconnection- Layer 1 (Physical Layer) Protocol Specification
STANAG 4262	The NATO Reference Model for Open Systems Interconnection - Layer 2 (Data Link Layer) Protocol Specification
STANAG 4263	The NATO Reference Model for Open Systems Interconnection - Layer 3 (Network Layer) Protocol Specification
STANAG 4271	ECM Resistant Digital Traffic Exchange Between Tactical Satellite Communications Terminals
STANAG 4285	Characteristics of a 1200/2400 Bits Per Second Single Tome Modulator/Demodulator for HF Radio Links
STANAG 4290	NATO Multi-Channel Tactical Digital Gateway - Cable Link (Optical) Standards
STANAG 4291	Modulation and Coding Characteristics that must be Common To Assure Interoperability of 2400 BPS Wireline Modems for Use in Narrow-Band Secure Voice Systems
STANAG 4292	Standards to Achieve Communications Between Tactical Combat Net Radio Equipment Designed to STANAG 4202 and Frequency Hopping Radios Operating in the Same VHF Band
STANAG 4295	Significant Data and Telegraph Signalling Conditions
STANAG 5000	Interoperability of Tactical Digital Facsimile Equipment
STANAG 5004	Military Characteristics for Field Telephone Sets (Minimum Standard)
STANAG 5009	(Exact Title Unknown - Relates to Naval Gunfire Support Using HF Radio)

STANAG 5018	NATO Manual Interface Between the Manual Switched Telecommunications Systems of the Combat Zone
STANAG 5020	Interoperability of Aircraft UHF Multi-Frequency Transceiver Installation and Compatible Ground Transmitters and Receivers
STANAG 5026	Military Characteristics for Facsimile Equipment To Meet Meteorological Requirements
STANAG 5028	Significant Telegraph Signalling Conditions in Automatic Telegraphy [Morse and International Alphabet (IA) No. 2]
STANAG 5030	Single and Multichannel VLF and LF On-Line Broadcast and Off-Line OOK Systems
STANAG 5031	Introduction of Modern Audio Equipment for Naval HF-MF and LF Shore-to-Ship Broadcasts
STANAG 5032	HF Single Sideband Single Channel Voice Communications (exact title unknown)
STANAG 5035	Introduction of an Improved System for Maritime Air Communications on HF, LF and UHF
STANAG 5036	Parameters and Practices for the Use of the NATO 7-Bit Code
STANAG 5038	Interoperability of Ship UHF Transmitting and Receiving Systems
STANAG 5040	NATO Automatic and Semi-Automatic Interfaces Between the National Switched Telecommunications Systems of the Combat Zone and Between These Systems and the NICS from 1979 to the 1990's
STANAG 5500	NATO Message Text Formatting System (FORMETS), ADSIA WG5 (see ADatP-3)
STANAG 5501	Tactical Data Exchange - Link 1 (Point-to-Point), ADISA WG4
STANAG 5504	Tactical Data Link for the Control of Aircraft - Link 4, ADISA WG4
STANAG 5505	NATO Standard Bit Fields, Bit Field Fillers and Codes
STANAG 5506	Link 6 SAM/NADGE Link
STANAG 5507	Tactical Data Link for Air Traffic Control - Link 7, ADISA WG4 (dormant)
STANAG 5510	Maritime Tactical Data Exchange - Link 10
STANAG 5511	Tactical Data Exchange - Link 11 and Link 11B, Volumes I and II, ADISA WG1
STANAG 5514	Tactical Data Broadcasting - Link 14, ADISA WG1
STANAG 5516	Tactical Data Exchange - Link 16, ADISA WG4
STANAG 5550	NATO Standard Data Elements, Data Items and Codes
STANAG 5601	Standards for Interface of NATO Data Links 1, 11, 14, and 11B Through a Ship/Shore/Ship Buffer, ADISA WG4
STANAG 5616	Standards for Data Forwarding Between Tactical Data Systems Employing Digital Data Link 11/11B and Tactical Data Systems Employing Link 16 (complementary to STANAG 4175)
STANAG 5620	Standards for the Interoperability of ADP Fire Support Systems
STANAG 5621	Standards for the Interoperability of NATO Land Combat and Combined Operations Systems
STANAG 5622	Air Operations System
STANAG 5623	Standards for Interoperability of Maritime Operations Systems

C. OTHER NATO DOCUMENTS

ACP 127	Message Relay Procedures
ACP 167(F)	Glossary of Communications-Electronics Terms, NATO, August 1981, UNCLASSIFIED
ADatP-2(D)	NATO Glossary of Automatic Data Processing (ADP) Terms and Definitions, December 1985, NATO UNCLASSIFIED
ADatP-3 (STANAG 5500)	NATO Message Text Formatting Systems, Part IV, Catalog of Standard Field Formats, December 1986, NATO UNCLASSIFIED
AM 96-1-4	Data Management, SHAPE, 30 October 1988, NATO UNCLASSIFIED
Classification Guide	NATO Network Security Information Classification Guide (NU), Version 1.0, TSGCE SG9, February 1989, NATO RESTRICTED
MC[4] 203/2	The Operational Requirements for the Interoperability of the Communications Between Different National Component Land Forces in the Combat Zone and the Communication Used in Provision of Air and Naval Support to These Forces
MC 277	The Operational Requirements for the Interoperability of Tactical Communication Systems for Use by the NATO Nations in the Land Combat Zone - Post 1985
MC 283	The Military Police for ECCM Applied to Tactical Communications in the Combat Zone
MC 284	The NATO Military Requirement for ECM Resistant and Secure Communications (NR)
NIMP	NATO Interoperability Management Plan (NIMP), Third Endorsement Edition, ADSIA-RCU-D/1 (Revised), Allied Data Systems Interoperability Agency, 1 July 1988, NATO UNCLASSIFIED
NIPD Vol. 1	NATO Interoperability Planning Document (NIPD), Volume 1, Introduction to Information Systems Interoperability Including the Allied Data Systems Interoperability Agency and the Organization of and Coordination Among NATO Bodies Involved in NATO Common Interoperability Standards Development and Configuration Management, Second Draft, ADSIA-RCA-WP/76, 20 April 1990, NATO UNCLASSIFIED

[4] MC: Military Characteristic

NIPD Vol. 2	NATO Interoperability Planning Document (NIPD), Volume 2, Formal Specification of Information Exchange Requirements, Draft, ADSIA-RCA-WP/72, February 1990, NATO UNCLASSIFIED
NIPD Vol. 3	NATO Interoperability Planning Document (NIPD), Volume 3, Plan for Development of NATO Common Interoperability Standards (NCIS), Revised Draft, ADSIA-RCA-WP/73 (First Revise), February 1990, NATO UNCLASSIFIED
NIPD Vol. 4	NATO Interoperability Planning Document (NIPD), Volume 4, NATO Common Interoperability Standards Configuration Management Plan (NCISCMP), Revised Draft, ADSIA-RCA-WP/32 (5th Revise), August 1989, NATO UNCLASSIFIED
NIPD Vol. 5	NATO Interoperability Planning Document (NIPD), Volume 5, NATO Common Interoperability Standards Testing Concept, First Draft, ADSIA-RCA-WP/75, February 1990, NATO UNCLASSIFIED
NIPD Vol. 6	NATO Interoperability Planning Document (NIPD), Volume 6, Documentation Plan for NATO Common Interoperability Standards, First Draft, ADSIA-RCA-D-15-90, 13 June 1990, NATO UNCLASSIFIED
NOSA	NATO OSI Security Architecture (NOSA), Ad Hoc Working Group on Security, TSGCE SG9, Draft Version 2.1, March 1988, NATO UNCLASSIFIED
NOSIP Strategy	NATO Open Systems Interconnection Profile (NOSIP) Strategy, TSGCE SG9, 23 September 1993, NATO UNCLASSIFIED
NTIS Transition Strategy	NATO Technical Interface Standards (NTIS) Transition Strategy, Sixth Edition, AC/259-D/1218(Revised), Conference of National Armaments Directors (CNAD), Tri-Service Group on Communications and Electronic Equipment (TSGCE), NATO, Brussels, September 1991, NATO UNCLASSIFIED
SANISI	Security Architecture for NATO Information Systems Interconnection (SANISI) (NU), Version 2.0, Ad Hoc Working Group on Security, TSGCE SG9, AC/302(SG/9)D/53, 14 April 1989, NATO CONFIDENTIAL
STAMINA 4.0	Standard Automated Message Interface for NATO ACCIS (STAMINA), Version 4.0, NACISA, April 1990, NATO UNCLASSIFIED
TM-776	Data Management Standardization for ACE ACCIS, TM-776, SHAPE Technical Centre, July 1985, NATO UNCLASSIFIED.

II. NATIONAL MILITARY STANDARDS

A. US DoD STANDARDS—GENERAL

DoD-STD-498	Software Development Standard (SDD), to be issued in 1994
DoD-STD-1467	Software Support Environment, 18 January 1985
DoD-STD-1700	Data Management Program, 28 September 1987
DoD-STD-1703	Software Product Standards, 12 February 1987
DoD-STD-1838A	Common Ada Programming Support Environment (APSE) Interface Set (CAIS-A), 6 April 1989
DoD-STD-2167A	Defense System Software Development
MIL-A-89007	Presentation Manager
MIL-ACQ-GUIDEA	Acquisition Guide for Implementation of Computer-aided Acquisition and Logistic Support (CALS)
MIL-C-28748A	Connectors, Electrical, Rectangular, Rack and Panel, Solder-Type and Crimp-Type Contacts, February 1985
MIL-C-CITIS	Contractor Integrated Technical Information Service (CITIS), Functional Requirements (Draft)
MIL-D-28000A	Digital Representation for Communication of Product Data: IGES Application Subsets, 10 February 1992 with Amendment 1 of 14 December 1992 (used in CALS for computer-aided design and vector graphics (e.g., in technical manual illustrations, engineering diagrams)
MIL-D-28003A	Digital Representation for Communication of Illustration Data: CGM Application Profile, 15 November 1991. Amendment 1 is dated 14 August 1992
MIL-D-87269	Interchange Formats for Interactive Electronic Technical Manual (IETM) Databases
MIL-D-89000	Digital Terrain Elevation Data
MIL-HDBK-59B	Department of Defense Computer-aided Acquisition and Logistic Support (CALS) Program Implementation Guide, 12 June 1993
MIL-HDBK-759B	Human Factors Engineering Design for Army Materiel Metric, June 1992
MIL-HDBK-761A	Human Engineering Guidelines for Management Information Systems, September 1989
MIL-HDBK-782	Software Support Environment Acquisition Implementation Guide for DoD-STD-2167, 29 February 1988
MIL-HDBK-829-1	MIL-STD-2045 Series Documentation, Volume 1, 23 April 1993
MIL-HDBK-829-2	Guidelines for Data Communications Protocol Standards (DCPS) DoD Standardized Profiles (DSPs), 23 April 1993
MIL-HDBK-1300	National Imagery Transmission Format Standard (NITFS), 18 June 1993
MIL-M-28001B	Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text and Amendment 1, 26 June 1993 (based on ISO 8879, SGML)
MIL-M-87268	Interactive Electronic Technical Manuals (IETMs): General Content, Style and Format
MIL-Q-87270	Requirements for Quality Assurance Programs for Interactive Electronic Technical Manuals (IETMs)
MIL-R-28002B	Requirements for Raster Graphics Representation in Binary Format, 14 December 1992 (based on GRP 4 Raster de facto industrial standards; used in CALS for Raster-scanned images in engineering drawings and technical manual illustrations)

B. US DoD STANDARDS—MIL-STD-2045-SERIES FOR DoD COMMUNICATIONS[5]

1000-Series—Physical Layer

2000-Series—Data Link Layer

3000-Series—Network Layer

3500-Series—Network/Relay Profiles/Multi-Layer

MIL-STD-1745-13500	Information Technology - Defense Standardized Profiles - Internet Relay Profile for DoD Communications - Point-to-Point Protocol (PPP), Working Draft, Draft, 1993

4000-Series—Transport Layer

4500-Series—Transport Profiles/Multi-Layer

MIL-STD-1745-14500	Reliable End System (ES) Transport for DoD Communications, Draft, 1993 (approved by DTMP for validation)
MIL-STD-1745-14501	Information Technology - Defense Standardized Profiles - Simplex Transport Profile (in SD-1 coordination[6])
MIL-STD-1745-14502-01	Information Technology - Defense Standardized Profiles - Internet Transport Profile for DoD Communications, Part 1: Transport and Internet Services, Draft, 1993 (in SD-1 coordination)
MIL-STD-1745-14502-02	Information Technology - Defense Standardized Profiles - Internet Transport Profile for DoD Communications, Part 2: Point-to-Point Links, Draft, 1993 (in SD-1 coordination)

---

5 These standards are being developed by the US DCPS Technical Management Panel (DTMP). This list was updated based on a private communication from JIEO/TBBD (Mr. Walt Lucchesi) on 10 January 1994, *DCPS MIL-STAN-2045 Number Assignments*, whose effective date was 13 December 1993.

6 Standerdardization Directory (SD-1) coordination is conducted to provide a baseline (incorporating comments from SD-1 coordination) for formal validation prior to final approval and publiccation.

MIL-STD-1745-14502-03 Information Technology - Defense Standardized Profiles - Internet Transport Profile for DoD Communications, Part 3: Wide Area Network Access, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-14502-04 Information Technology - Defense Standardized Profiles - Internet Transport Profile for DoD Communications, Part 4: Local Area Network (LAN) Media Independent Requirements, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-14502-05 Information Technology - Defense Standardized Profiles - Internet Transport Profile for DoD Communications, Part 5: Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) Local Area Network (LAN) Media Dependent Requirements, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-14502-06 Information Technology - Defense Standardized Profiles - Internet Transport Profile for DoD Communications, Part 6: Combat Net Radio, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-44500 Tactical Communications 2 (TACO2), Draft, 1993 (sent to Navy publications)

5000-Series—Session Layer

6000-Series—Presentation Layer

7000-Series—Application Layer

7500-Series—Application Profiles/Multi-Layer[7]

MIL-STD-1745-17501-01 Information Technology - Defense Standardized Profiles AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 1: MHS Service Support, Draft, 1993 (sent to Navy publications)

MIL-STD-1745-17501-02 Information Technology - Defense Standardized Profiles AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 2: Specification of ROSE, RTSE, ACSE, Presentation and Session Protocols for use by DoD MHS, Draft, 1993 (sent to Navy publications)

MIL-STD-1745-17501-03 Information Technology - Defense Standardized Profiles AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 3: Requirements for Message Transfer (P1), Draft, 1993 (sent to Navy publications)

MIL-STD-1745-17501-04 Information Technology - Defense Standardized Profiles AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 4: Messaging Requirements for MTS Access (P3), Draft, 1993 (sent to Navy publications)

MIL-STD-1745-17501-05 Information Technology - Defense Standardized Profiles AMH 1n (D)- Message Handling System (MHS) Common Messaging, Part 5: Messaging Requirements for MS Access (P7), Draft, 1993 (sent to Navy publications)

MIL-STD-1745-17502 MHS Military Messaging, Content Type AMH 2n (D), Draft, 1993 (baseline for validation; requesting approval to publish from DTMP)

MIL-STD-1745-17503-01 Information Technology - Defense Standardized Profiles - Internet Message Transfer Profile for DoD Communications, Part 1: Simple Mail Transfer Protocol (in SD-1 coordination)

MIL-STD-1745-17503-02 Information Technology - Defense Standardized Profiles - Internet Message Transfer Profile for DoD Communications, Part 2: Format of Text Messages, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17504 Information Technology - Defense Standardized Profiles - Internet File Transfer Profile for DoD Communications, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17505 Information Technology - Defense Standardized Profiles - Internet Domain Name Service (DNS) Profile for DoD Communications, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17506 Information Technology - Defense Standardized Profiles - Internet Remote Login Profile for DoD Communications, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17507-01 Information Technology - Defense Standardized Profiles - Internet Network Management Profile for DoD Communications, Part 1: Simple Network Management Protocol (SNMP), Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17507-02 Information Technology - Defense Standardized Profiles - Internet Network Management Profile for DoD Communications, Part 2: Management Information Base (MIB), Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17507-03 Information Technology - Defense Standardized Profiles - Internet Network Management Profile for DoD Communications, Part 3: Structure and Identification of Management Information, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17508-01 Information Technology - Defense Standardized Profiles AFT 1n (D) - File Transfer, Access and Management, Part 1: Specification of ACSE, Presentation and Session Protocols for Use by FTAM, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17508-02 Information Technology - Defense Standardized Profiles AFT 1n (D) - File Transfer, Access and Management, Part 2: Definition of Document Types, Constraint Sets and Syntaxes, Draft, 1993 (in SD-1 coordination)

---

7 The US Joint Interoperability Test Center (JITC) has completed validation testing of MIL-STD-2045-17501 and -17502. Some minor deficiencies were noted, and the DTMP has approved these for publication with these corrections.

MIL-STD-1745-17508-03 Information Technology - Defense Standardized Profiles AFT 1n (D) - File Transfer, Access and Management, Part 3: AFT 11—Simple File Transfer Service (Unstructured), Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17508-04 Information Technology - Defense Standardized Profiles AFT 1n (D) - File Transfer, Access and Management, Part 4: AFT 12—Positional File Transfer Service for Flat Files, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17508-05 Information Technology - Defense Standardized Profiles AFT 1n (D) - File Transfer, Access and Management, Part 5: AFT 22—Positional File Access Service for Flat Files, Draft, 1993 (in SD-1 coordination)

MIL-STD-1745-17508-06 Information Technology - Defense Standardized Profiles AFT 1n (D) - File Transfer, Access and Management, Part 6: AFT 3—File Management Service, Draft, 1993 (in SD-1 coordination)

8000-Series—Network Management

MIL-STD-1745-38000 Government Network Management Profile (GNMP), 1991 (approved and published)

MIL-STD-1745-38000 DoD Network Management for DoD Communications, Version 2 of GNMP, Draft (working group circulation), DTMP/WG3, 1992

8500-Series—Security[8]

MIL-STD-1745-18500-01 Information Technology - Defense Standardized Profiles AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 1: MSP Service Support, Draft, DTMP/WG3, 1993 (sent to Navy publications)

MIL-STD-1745-18500-02 Information Technology - Defense Standardized Profiles AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 2: MSP Content Protocol, Draft, DTMP/WG3, 1993 (sent to Navy publications)

MIL-STD-1745-18500-03 Information Technology - Defense Standardized Profiles AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 3: MSP Requirements for Message Transfer, Draft, DTMP/WG3, 1993 (sent to Navy publications)

MIL-STD-1745-18500-04 Information Technology - Defense Standardized Profiles AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 4: MSP Requirements for MS Access, Draft, DTMP/WG3, 1993 (sent to Navy publications)

MIL-STD-1745-18500-05 Information Technology - Defense Standardized Profiles AMH Xn (D)- Message Handling System (MHS) Message Security Protocol, Part 5: MSP Requirements for MS Access, Draft, DTMP/WG3, 1993 (sent to Navy publications)

MIL-STD-1745-48501 Common Security Label, Draft, 1993 (in SD-1 coordination)

MIL-HDBK-Series

MIL-HDBK-829-1 (Vol 1) *MIL-STD-2045-Series Documentation*, Volume 1, DTMP/WG5, 23 April 1993 (published)

MIL-HDBK-829-2 (Vol 2) Guidelines for Data Communications Protocol Standards (DCPS) DoD Standardized Profiles (DSPs), Volume 2, DTMP/WG5, 23 April 1993 (published)

MIL-HDBK-1350-1 (Vol 1) Validation of Data Communications Protocol Standards for Military Applications, DTMP/WG7, Draft, 1993 (requesting DTMP approval for SD-1 coordination)

MIL-HDBK-1350-2 (Vol 2) Data Communications Protocol Conformance and Interoperability Testing and Registration, DTMP/WG7, Draft, 1993 (requesting DTMP approval for SD-1 coordination)

MIL-HDBK-1351 Network Management for DoD Communications, DTMP/WG4, 23 July 1993 (sent to Navy publications)

C. US DoD STANDARDS—OTHER MIL-STDs

MIL-STD-188-114A Electrical Characteristics of Digital Interface Circuits, July 1984

MIL-STD-188C Military Communication System Technical Standards, November 1969

MIL-STD-188-100 Common Long-Haul and Tactical Communication System Technical Standards, November 1972

MIL-STD-188-148(S) Interoperability Standards for Anti-Jam Communications in the HF Band (U)

MIL-STD-188-196 Bi-Level Image Compression for the National Imagery Transmission Format Standard, 18 June 1993

MIL-STD-188-197 Adaptive Recursive Interpolated Differential Pulse Code Modulation (ARIDPCM) Compression Algorithm for the National Imagery Transmission Format Standard, 18 June 1993

MIL-STD-188-220 Interoperability Standard for Digital Message Transfer Device (DMTD) Systems, 1993 (approved and published)

MIL-STD-198 Joint Photographic Experts Group (JPEG) Image Compression for National Imagery Transmission Format Standard, 18 June 1993

MIL-STD-974 Contractor Integrated Technical Information Service (CITIS), Fall 1993

MIL-STD-1379D Military Training Programs

MIL-STD-1388-2B DoD Requirements for a Logistic Support Analysis Record

MIL-STD-1472D Human Engineering Design Criteria for Military Systems, Equipment and Facilities, March 1989

MIL-STD-1777 Internet Protocol (IP), August 1983

---

8 MIL-STD-2045-18500 has been validated by the US JITC.

MIL-STD-1778	Transmission Control Protocol (TCP), August 1983
MIL-STD-1779	Interfaces for High Capacity C3 Local Area Networks, November 1983
MIL-STD-1780	File Transfer Protocol (FTP), May 1984
MIL-STD-1781	Simple Mail Transfer Protocol (SMTP), May 1984
MIL-STD-1782	TELENET Protocol, May 1984
MIL-STD-1800A	Human Engineering Performance Requirements for Systems, October 1990
MIL-STD-1801	User/Computer Interface, May 1987
MIL-STD-1815A	Ada Programming Language (ISO 8652), 1983
MIL-STD-1840B	Automated Interchange of Technical Information, 3 November 1992
MIL-STD-2045-44500	Tactical Communications Protocol 2 (TACO2) for National Imagery Transmission Format Standard, 18 June 1993
MIL-STD-2167A	Defense System Software Development Standard
MIL-STD-2168	Defense System Software Quality Program
MIL-STD-2301	Computer Graphics Metafile (CGM) Implementation Standard for the National Imagery Transmission Format Standard, 18 June 1993
MIL-STD-2500	National Imagery Transmission Format (Version 2.0) for the National Imagery Transmission Format Standard, 18 June 1993
MIL-STD-7035A	Defense System Software Documentation Standard
MIL-STD-SDS	Defense System Software Development and Documentation Standard
MIL-T-31000	General Specifications for Technical Data Packages (supersedes DoD-D-1000, Engineering Drawings and Associated Lists)

D. US DoD STANDARDS—DoD INTERNET REQUESTS FOR COMMENT (RFCs)

RFC[9] 742	Finger Protocol (Elective, Proposed Standard)
RFC 768	User Datagram Protocol (UDP) (Recommended)
RFC 783	Trivial File Transfer Protocol (TFTP) (Elective, Draft Standard)
RFC 791	Internet Protocol (IP) (Required)
RFC 792	Internet Control Message Protocol (ICMP) (Required)
RFC 793	Transmission Control Protocol (TCP) (Recommended)
RFC 821	Simple Mail Transfer Protocol (SMTP) (Recommended)
RFC 822	Format of Electronic Mail Messages (MAIL) (Recommended)
RFC 826	Address Resolution Protocol (ARP) (Elective)
RFC 854	TELNET Protocol (Recommended)
RFC 862	Echo Protocol (ECHO) (Recommended)
RFC 863	Discard Protocol (DISCARD) (Elective)
RFC 864	Character Generator Protocol (CHARGEN) (Elective)
RFC 865	Quote of the Day Protocol (QUOTE) (Elective)
RFC 866	Active Users Protocol (USERS) (Elective)
RFC 867	Daytime Protocol (DAYTIME) (Elective)
RFC 868	Time Server Protocol (TIME) (Elective)
RFC 877	Internet Protocol on X.25 Networks (IP-X25) (Elective)
RFC 891	Internet Protocol on DC Networks (IP-DC) (Elective)
RFC 894	Internet Protocol on Ethernet Networks (IP-E) (Elective)
RFC 895	Internet Protocol on Experimental Ethernet Networks (IP-EE) (Elective)
RFC 903	A Reverse Address Resolution Protocol (RARP) (Elective)
RFC 904	Exterior Gateway Protocol (EGP) (Recommended)
RFC 907	Internet Protocol on Wideband Networks (IP-WB) (Elective)
RFC 919	Internet Protocol Broadcast Datagrams (Required)
RFC 922	Internet Protocol Broadcast Datagrams With Subnets (Required)
RFC 950	Internet Protocol Subnet Extension (Required)
RFC 951	Bootstrap Protocol (BOOTP)
RFC 954	Who Is Protocol NICNAME) (Elective, Draft Standard)
RFC 959	File Transfer Protocol (FTP) (Recommended)
RFC 1001-1002	Net BIOS Service Protocol (Elective)
RFC 1006	ISO Transport Service on Top of TCP (TP-TCP) (Elective, Draft Standard)
RFC 1009	Gateway Requirements (Required)
RFC 1034-1035	Domain Name System (Recommended)
RFC 1042	Internet Protocol on IEEE 802 (IP-IEEE) (Elective)
RFC 1044	Internet Protocol on Hyperchannel Networks (IP-HC) (Elective)

9 The list of Internet Requests for Comment (RFCs) was updated from the Internet Information Services, RFC Directory, available on DMSOPROTO, September 1993

RFC 1048	Bootstrap Protocol (BOOTP) (Recommended, Draft Standard)
RFC 1049	Content of Header Type (CONTENT) (Recommended)
RFC 1051	Internet Protocol on ARCNET (IP-ARC) (Elective)
RFC 1054	Internet Group Multicast Protocol (IGMP)
RFC 1055	Transmission of IP Over Serial Lines (IP-SLIP) (Elective)
RFC 1058	Routing Information Protocol (RIP) (Elective, Draft Standard)
RFC 1059	Network Time Protocol
RFC 1060	Assigned Numbers (Required)
RFC 1084	Bootstrap Protocol (BOOTP) (Recommended, Draft Standard)
RFC 1088	Transmission of IP Over NetBIOS (IP-NETBIOS) (Elective)
RFC 1095	Common Management Information Services and Protocol Over TCP/IP (CMOT) (Recommended, Draft Standard)
RFC 1103	Transmission of IP Over FDDI (IP-FDDI) (Elective)
RFC 1112	Internet Group Multicast Protocol (IGMP) (Recommended)
RFC 1113-15	Mail Privacy (Procedures, Key Management, and Algorithms) (Elective, Draft Standard)
RFC 1122	Host Requirements--Communications (Required)
RFC 1123	Host Requirements--Applications (Required)
RFC 1132	Transmission of 802.2 over IPX Nets (IP-IPX (Elective)
RFC 1155	Structure of Management Information (SMI) (Recommended)
RFC 1156	Management Information Base (MIB) (Recommended)
RFC 1157	Simple Network Management Protocol (SNMP) (Recommended)
RFC 1165	Network Time Protocol (NTP) over the OSI Remote Operations Service
RFC 1171	Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams over Point-to-Point Links, D. Perkins, July 1990
RFC 1172	The Point-to-Point Protocol (PPP) Initial Configuration Options, D. Perkins and R. Hobby, 1990
RFC 1174	IAB recommended policy on distributing internet identifier assignment and IAB recommended policy change to internet "connected" status
RFC 1176	Interactive Mail Access Protocol: Version 2
RFC 1179	Line printer daemon protocol.
RFC 1188	Proposed standard for the transmission of IP datagrams over FDDI networks
RFC 1189	Handspicker, B. Common Management Information Services and Protocols for the Internet (CMOT and CMIP)
RFC 1190	Experimental Internet Stream Protocol: Version 2 (ST-II)
RFC 1191	Path MTU discovery
RFC B1822	Internet Protocol on ARPANET IIP-ARPA) (Elective)
RFC 1203	Interactive Mail Access Protocol: Version 3
RFC 1204	Message Posting Protocol (MPP)
RFC 1220	Point-to-Point Protocol Extensions for Bridging
RFC 1221	Host Access Protocol (HAP) specification: Version 2
RFC 1223	OSI CLNS and LLC1 protocols on Network Systems HYPERchannel.
RFC 1225	Post Office Protocol: Version 3
RFC 1227	SNMP MUX protocol and MIB
RFC 1228	SNMP-DPI: Simple Network Management Protocol Distributed Program Interface
RFC 1235	Coherent File Distribution Protocol
RFC 1237	Guidelines for OSI NSAP Allocation in the Internet, R. Colella, E. P. Gardner, and R. W. Callon, July 1991
RFC 1240	OSI connectionless transport services on top of UDP: Version 1
RFC 1241	Scheme for an internet encapsulation protocol: Version 1
RFC 1244	Site Security Handbook
RFC 1247	OSPF version 2
RFC 1249	DIXIE protocol specification
RFC 1253	OSPF version 2: Management Information Base
RFC 1267	A Border Gateway Protocol 3 (BGP-3)
RFC 1281	Guidelines for the Secure Operation of the Internet
RFC 1288	The Finger User Information Protocol
RFC 1293	Inverse Address Resolution Protocol
RFC 1301	Multicast Transport Protocol
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
RFC 1307	Dynamically Switched Link Control Protocol
RFC 1331	The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links
RFC 1332	The PPP Internet Protocol Control Protocol (IPCP)
RFC 1334	PPP Authentication Protocols

RFC 1339	Remote Mail Checking Protocol
RFC 1350	THE TFTP PROTOCOL (REVISION 2), (Obsoletes RFC 783)
RFC 1352	SNMP Security Protocols
RFC 1361	Simple Network Time Protocol (SNTP)
RFC 1376	The PPP DECnet Phase IV Control Protocol (DNCP)
RFC 1377	The PPP OSI Network Layer Control Protocol (OSINLCP), November 1992
RFC 1378	The PPP AppleTalk Control Protocol (ATCP)
RFC 1385	EIP: The Extended Internet Protocol A Framework for Maintaining Backward Compatibility
RFC 1388	RIP Version 2 - Carrying Additional Information
RFC 1411	Telnet Authentication: Kerberos Version 4
RFC 1413	Identification Protocol
RFC 1415	FTP-FTAM Gateway Specification
RFC 1418	SNMP over OSI
RFC 1419	SNMP over AppleTalk
RFC 1421	Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, (Obsoletes RFC 1113)
RFC 1422	Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management
RFC 1423	Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers
RFC 1424	Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services
RFC 1425	SMTP Service Extensions
RFC 1426	SMTP Service Extension for 8-bit-MIME transport
RFC 1429	Listserv Distribute Protocol
RFC 1434	Data Link Switching: Switch-to-Switch Protocol
RFC 1436	The Internet Gopher Protocol

III. AGREEMENTS FROM REGIONAL WORKSHOPS

ED 024	Application Function A/713, Behavior of DSAs for Distributed Operations, European Workshop for Open Systems, [EWOS EGDIR/91/29], Final Draft, February 1991
EWOS/ETG003	EWOS/EG FT, File Transfer Access and Management - FTAM Remote Actions (RA) Service and Protocol, 24 January 1990
EWOS/EG VT/89	Application Function A/4121, Basic Class VT S-Mode Forms Functional Standard, Part 1: Virtual Terminal Service, EWOS/EG VT/89/53, Part 2: VT Protocol Check List, EWOS/EG VT/89/59, and Part 3: Underlying Layers Check List, EWOS/EG VT/89/60, Final Text, prENV 41 208
Profile RC p,q	X.25 Protocol Relaying, Draft, EWOS/EGLL/2990/81, EWOS, 9 May 1990
ECMA TR/46	Security in Open Systems--A Security Framework, ECMA TR/46, European Computer Manufacturers Association, July 1988
ECMA TR/55	Reference Model for Frameworks on Computer Assisted Software Engineering Environments, developed by ECMA TC33 Technical Group on Reference Models (TGRM), December 1990.
E..MA 149	Portable Common Tools Environment (PCTE) Abstract Specification, European Computer Manufacturers Association, December 1990
ECMA 158	Portable Common Tools Environment (PCTE) C Programming Language Binding, European Computer Manufacturers Association, June 1991
ECMA 162	PCTE Ada Program Language Binding, December 1991
ENV[10] 41 101	LANs: Provision of the OSI Connection-Mode Transport Service (COTS) Servic. .ing the Connectionless-Mode Network Service (CLNS) on a CSMA/CD Single LAN, June 1986
ENV 41 102	LANs: Provision of the OSI COTS and the CLNS on a CSMA/CD Single or Multiple LAN Configuration, June 1986
ENV 41 103	LANs: Provision of the OSI COTS and the Connection-Mode Network Service (CONS) in an End System on a CSMA/CD LAN, August 1990
ENV 41 104	Packet Switched Data Networks: Permanent Access, August 1987
ENV 41 105	Packet Switched Data Networks: Switched Access, June 1988
ENV 41 106	Digital Data Circuit (CSDN) - Provision of the OSI COTS in the T.70 Case for Telematic End Systems, June 1988
ENV 41 107	Digital Data Circuit (CSDN) - Provision of the OSI COTS and the OSI CONS, June 1988
ENV 41 108	LANs: Provision of the OSI COTS and CONS in an End System on a Token Ring LAN, August 1990
ENV 41 109	LANs: Provision of the OSI COTS Using CLNS on a Token Ring Single LAN, February 1988
ENV 41 110	LANs: Provision of the OSI COTS Using CLNS in an End System on a Token Ring LAN in a Single or Multiple LAN Configuration, February 1988
ENV 41 111	ISDN: X.25 DTE to DTE Operation (B-channel)
ENV 41 112	ISDN: X.25 DTE to DTE Operation (Circuit-mode service)
ENV 41 201	Private Message Handling System - User Agent and Message Transfer Agent; Private Management Domain to Private Management Domain, June 1986
ENV 41 202	Message Handling Systems; User Agent and Message Transfer Agent: Access to an Administration Management Domain (ADMD), August 1987
ENV 41 203	Exchange of Telex Documents Between Two End Systems, Which May Be Teletex Terminals, June 1988
ENV 41 204	FTAM: Simple File Transfer, September 1989
ENV 41 205	FTAM: File Management, June 1989
ENV 41 206	FTAM: Positional File Transfer, September 1989
ENV 41 207	FTAM: Positional File Access Service, September 1989
ENV 41 208-1	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 1: Virtual Terminal Service, European Prestandard, December 1990
ENV 41 208-2	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms - Part 2: Check List, European Prestandard, December 1990
ENV 41 208-3	Information System Interconnection - Basic Class Virtual Terminal - S-mode Forms Part 3: Underlying Layers Checklist, European Prestandard, December 1990
ENV 41 209	Information System Interconnection - Basic Class Virtual Terminal - Common Control Objects, European Prestandard, December 1990
prENV 41 210	Directory: Directory Access Protocol, April 1990
prENV 41 211-1	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode X.3 (A/VT15) - Part 1: Virtual Terminal Service, May 1991
prENV 41 211-2	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode X.3 (A/VT15) - Part 2: Virtual Terminal Protocol Checklist, May 1991

[10] ENV indicates a standard approved by the Join European Standards Institution (CEN/CENELEC) and the European Workshop for Open Systems (EWOS).

prENV 41 211-3	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode X.3 (A/VT15) - Part 3: Underlying Layers Checklist, May 1991
prENV 41 212	Information Systems Interconnection - Directory System Protocol (A/DI2), May 1991
prENV 41 213-1	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode 'Telnet' (A/VT13) - Part 1: Virtual Terminal Service, May 1991
prENV 41 213-2	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode 'Telnet' (A/VT13) - Part 2: Virtual Terminal Protocol Checklist, May 1991
prENV 41 213-3	Information Systems Interconnection - Virtual Terminal Basic Class - A-mode 'Telnet' (A/VT13) - Part 3: Underlying Layers Checklist, May 1991
ENV 41 504	Data Stream Formats, Character-coded Text, Telex-compatible
ENV 41 506	Data Stream Formats, Character-coded Text, Teletex-compatible
ENV 41 507	Data Stream Formats, Character-coded Text, Videotex-compatible
ENV 41 509	ODF: Simple Document Structure, Character Content Architecture Only, January 1989
ENV 41 510	ODF: Enhanced Document Structure, Character, Raster, Geometric Graphics Content Architecture, January 1989
ENV 41 511	ODF: Processable and Layout Independent Documents, Simple Messaging Profile, January 1989
prENV 41 512	Directory Data Definitions, Common Directory Use, April 1990
prENV 41 513	Information Systems Interconnection - Virtual Terminal Basic Class - VT Font Assignment Type 1 (F/441), July 1991
ENV 41 901	X.29-Mode Procedures Between a Packet Mode DTE or a PAD and a PAD via a Public or Private X.25 Packet Switched Network or ISO 8208 Packet Level Entity and ISO 7776 Link Level Entity, June 1987
prETS 300 383	Integrated Services Digital Network (ISDN): File Transfer over the ISDN (Using the) EUROFILE Transfer Profile, ETSI, December 1993
prETS 300 388	Integrated Services Digital Network (ISDN): File Transfer and Access Management (FTAM) over ISDN Based on Simple File Transfer Profile, ETSI, December 1993
IGOSS	The Industry/Government Open Systems Specification (IGOSS), Draft, IGOSS Panel, January 1994 (expected to be published as Version 1 in 1994; IGOSS is a joint effort by the US Government, the Canadian Government, MAP Users Group, TOP Users Group, and the Electric Power Research Institute)
MAP	Manufacturing Automation Protocol (MAP), World Federation of MAP/TOP Users Groups (distributed by the Corporation for Open Systems)
M-IT-01	The Concept of Profiles and Structure for Functional Standards for Information Technology, Adopted by CEN/CENELEC/ETSI ITSTC, 1991
M-IT-02	Taxonomy of Profiles and Directory of Functional Standards (For Interworking in an OSI Environment) Adopted by CEN/CENELEC/ETSI ITSTC, 1991
M-IT-03	A Framework for Testing and Certification in Europe (being implemented by ECITC)
NIST SP 500-206	Stable Implementation Agreements (SIA) for Open Systems Interconnection Protocols, Version 6, Proceedings of the December 1992 NIST OSE Implementor's Workshop (OIW), March 1993
NIST SP 500-xxx	Stable Implementation Agreements (SIA) for Open Systems Interconnection Protocols, Version 7, Proceedings of the December 1993 NIST OSE Implementor's Workshop (OIW), January 1994 (electronic edition is available; publication is forthcoming)
NIST WIA-91	Working Implementation Agreements (WIA), Proceedings of the December 1991 NIST OSE Implementor's Workshop (OIW), March 1992
NIST WIA-93	Working Implementation Agreements (WIA), Proceedings of the December 1991 NIST OSE Implementor's Workshop (OIW), March 1994 (electronic edition is available; publication is forthcoming)
TOP	Technical Office Protocol (TOP), World Federation of MAP/TOP Users Groups (distributed by the Corporation for Open Systems)
X-Windows	X-Window System, X Version 11, Release 4 (X11-R4), M.I.T. X Consortium
Z39.50	Z.39.50 Implementors Group Profile, ANSI Z39.50-MA-026
EWOS Technical Guides	
EWOS ETG 001	FTAM - Tutorial on Rules for ASN.1 Encoding, April 1989
EWOS ETG 003	FTAM - Remote Actions (RA) over FTAM, Service and protocol, Edition 2, May 1992
EWOS ETG 005	Introduction to Directory Profiles, Edition 3, May 1993
EWOS ETG 007	FTAM - Service Classes and Functional Units in ENV 41 205, Edition 2, August 1990
EWOS ETG 008	Procedures and Evaluation Criteria for Standardization of Test Specifications for European Functional Standards, October 1990
EWOS ETG 009	Conformance Vocabulary, Edition 2, September 1992
EWOS ETG 010	Conformance Tutorial, January 1991
EWOS ETG 011	Tutorial for Directory Q-Profile Production, January 1991
EWOS ETG 013	A Mapping of the X-Window System over an OSI Stack, May 1991
EWOS ETG 016	PTS Specification, February 1992
EWOS ETG 017	Error Handling in Directory, May 1992
EWOS ETG 018	OSI TP Tutorial, Part 1, September 1992 and Part 2, May 1993 (separate volumes)

EWOS ETG 020	PTS Maintenance Procedures, September 1992
EWOS ETG 022	Organization of Common PTS, November 1992
EWOS ETG 025	The TTCN Style Guide and Quality Criteria, November 1993
EWOS ETG 026	Role of Standards in OSI Testing, Edition 2, February 1993
EWOS ETG 027	Security Architecture for the Directory, February 1993
EWOS ETG 028	Interoperability - Vocabulary, May 1993
EWOS ETG 029	Interoperability - Classification, May 1993
EWOS ETG xxx	Library of Test Specifications, Draft (ETG expected November 1993)
EWOS ETG xxx	Technical Guide to ISO 9646 Test Environment, Draft (ETG expected November 1993)
EWOS ETG xxx	Interconnection of Directory Domains (DMD-DMD), Draft (ETG expected November 1993)
EWOS ETG xxx	Methodology Handbook for PTS Production, Draft (replaces ETG 008; ETG expected February 1994)
EWOS ETG xxx	Test Report Proformas, Draft (ETG expected February 1994)
EWOS ETG xxx	Development of Taxonomy for DBE Requirements, Draft (ETG expected March 1994)
EWOS ETG xxx	Technical Framework for Security-Related Profile Development, Draft (ETG expected May 1994)
EWOS ETG xxx	Application of Security Techniques to Base Standards, Draft (ETG expected May 1994)
EWOS ETG xxx	User Requirements for More DBE Profiles, Draft (ETG expected September 1994)
EWOS ETG xxx	Policy Statement on the Role of Standards in OSI Testing, Draft
Regional Workshop Technical Reports	
RWS-TR 001	Guiding Principals for Regional Requirements
RWS-TR xxx	Guidelines for Managed Object Profiling and Taxonomy (EWOS), November 1993 (RWS-TR expected February 1994)
RWS-TR xxx	Framework for Conformance Testing of Network Management Profiles (EWOS), September 1993 (RWS-TR expected February 1994)
RWS-TR xxx	Registration of Object Identifiers in ISPs (EWOS SD-16; EWOS approval expected March 1994)
RWS-TR xxx	Conformance Testing Vocabulary (EWOS approval expected May 1994)
RWS-TR xxx	TTCN Style Guide (EWOS approval expected November 1994)
RWS-TR xxx	Library of Test Specifications (EWOS approval expected November 1994)
RWS-TR xxx	Guidelines for Managed Object Harmonization (EWOS approval expected November 1994)
RWS-TR xxx	Ensembles Guidelines (EWOS approval expected November 1994)
RWS-TR xxx	Test Case Selection Rules (OIW)
Regional Workshop Technical Paper	
EWOS TA/92/201	Vocabulary of Terms Used in Communication Protocols Conformance Testing, July 1992
EWOS TA/92/202	Framework for Conformance and Testing of Network Management Profiles, July 1992
EWOS TA/93/030	A Tutorial on Upper Layer Naming and Addressing, February 1993
EWOS TA/93/114	Upper Layer Naming and Addressing Management Summary, April 1993
EWOS TA/93/238	Final Report of Joint ETSI/PT 24V-EWOS/PT N 017: Guide for the Implementation of the ISO/IEC Conformance Assessment Process, July 1993
EWOS TA/93/239	Guidelines for Managed Object Taxonomy and Profiles, July 1993
EWOS TA/93/240	EWOS/EG-NM Statement of Intent about the Use of CULR Part 1 Document, August 1993
EWOS TA/93/255	Information and Documentation - Open Systems Interconnection - ISPs ALD 1n - Library and Documentation Search and Retrieve, Part 1: Specification of ACSE, Presentation, and Session Protocols for Use by ALD 1n, August 1993
EWOS TA/93/256	Information and Documentation - Open Systems Interconnection - ISPs ALD 2n - Library and Documentation Inter-Library Loan, Part 2: Inter-Library Loan Generic for ALD 2n, August 1993
EWOS TA/93/257	Information and Documentation - Open Systems Interconnection - ISPs ALD 2n - Library and Documentation Inter-Library Loan, Part 3: ALD 21, Inter-Library Loan Using Connection-Oriented ACSE, August 1993
EWOS TA/93/258	Framework for Conformance and Testing of OSI Management Profiles, August 1993
EWOS TA/93/300	Resolutions of EWOS/TA22, September 1993
EWOS TA/93/318	Annexes to the Draft Summary Report of EWOS/TA22, Brussels, 7-8 September 1993, September 1993
EWOS TA/93/320	Invitation to a Special Meeting on TCP/IP-OSI Convergence, EWOS, October 1993
EWOS TA/93/326	Report of the 15th EGN Meeting of 5-7 October 1993, October 1993
EWOS TA/93/327	Liaison to SGFS on Submission of AOM 2x Taxonomy, October 1993
EWOS TA/93/329	The TTCN Style Guide, EWOS Technical Guide 025, Revision 1, October 1993
EWOS TA/93/331	Proposal for EWOS EG EDI, Chairperson EWOS Ad Hoc Group on EDI, October 1993
EWOS TA/93/332	Proposed New Work Item for EG EDI, Profiling Methodologies for Composite EDI Message Structures, October 1993
EWOS TA/93/334	Proposed New Work Item for EG EDI, Interactive EDI and TP, October 1993
EWOS TA/93/350	Proposed New Work Item for EG CT, Interoperability Methodology Tracking, November 1993
EWOS TA/93/355	Proposed New Work Item for EG NM, ISO/Internet Management Coexistence Process, November 1993
EWOS TA/93/357	EWOS/TLG Draft Explanatory Report of pDISP 11188-2, Common Upper Layer Requirements, Part 2: Basic Connection-Oriented Requirements for ROSE-based Profiles, October 1993

EWOS TA/93/362	Draft Report of the 13th EWOS/EG-TP Meeting, Brussels, 5-7 October 1993, EWOS/EG-TP Secretariat, October 1993
EWOS TA/93/385	EWOS/TLG Report to TA23, 23-24 November 1993, EWOS/TLG Chair, October 1993
EWOS TA/93/391	EWOS/TA Session on TCP/IP-OSI Convergence/Coexistence, EWOS, October 1993
EWOS TA/93/399	Minimal OSI Upper Layers (mOSI) Portability and Convergence, Briefing by Jim Quigley, November 1993
EWOS TA/93/405	Annexes to the Draft Summary Report of EWOS/TA23, 23-24 November 1993, EWOS, December 1993
EWOS TA/93/424	Draft Minutes of the 20th Joint Meeting of EWOS/EG-DIR and ETSI STC TE. Held in Brussels 4-8 October 1993, EWOS/EG-DIR Secretariat, November 1993
EWOS TA/93/425	Seventh Meeting of the EWOS Expert Group on Database Enquiry 5-7 October 1993, Draft Report, EG-DBE, December 1993

IV. NATIONAL STANDARDS AND PAPERS

A. UK STANDARDS AND PAPERS

UK GOSIP Vol. 1	UK Government OSI Profile, Volume I, Introduction, Version 5, Central Computer and Telecommunications Agency, London, 1992
UK GOSIP Vol. 2	UK Government OSI Profile, Volume II, Specification, Version 5, Central Computer and Telecommunications Agency, London, 1992
UK GOSIP Vol. 3	UK Government OSI Profile, Volume III, Procurement Handbook, Version 5, Central Computer and Telecommunications Agency, London, 1992
Users Handbook	Users' Open Systems Handbook, Level-7 Limited, United Kingdom, 1989

B. CA STANDARDS AND PAPERS

CSA X243.110.2	Canadian OSI Registration Procedures and Guidelines, Part 2 Guidelines for Network Service Access Point Addresses for the Data Country Code Format

C. US STANDARDS AND PAPERS[11]

AIAA/ANSI G-009-1991	Guide for Implementing Software Development Files Conforming to DoD-STD-2167A, 1991
ANSI/AIIM MS53-1	File Format for Storage and Exchange of Images, Part 1, Bi-Level Image File Format, 1993
ANSI/AIIM MS53-2	File Format for Storage and Exchange of Images, Part 2, JPEG Image Coding, TBD in late 1993
ANSI/MIL 1815A	Reference Manual for the Ada Programming Language, 1983
ANSI/NISO Z39.50	Information Retrieval Application Service Definition and Protocol Specification for Open Systems Interconnection (formerly ANSI Z39.50-1988), 1992
ANSI/NISO Z39.58	Common Command Language for On-line Interactive Information Retrieval, 1992
ANSI/NISO Z39.59	Electronic Manuscript Preparation and Markup Standard, 1988
ANSI/NISO Z39.63	Interlibrary Loan Data Elements, 1989
ANSI/NISO Z39.67	Computer Software Description, 1993
ANSI/SMPTE RP 125	Digital Interface Standard, Draft
ANSI T1.101	Telecommunications - Synchronization Interface Standards for Digital Networks, 1987
ANSI T1.102	Telecommunications - Digital Hierarchy - Electronic Interfaces, 1987
ANSI T1.103	Telecommunications - Digital Hierarchy - Synchronous DS3 Format Specifications, 1987
ANSI T1.103a	Telecommunications - Digital Hierarchy - Synchronous DS3 Format Specifications, 1990
ANSI T1.104	Telecommunications - Exchange-Interexchange Carrier Interfaces - Individual Channel Signaling Protocols, 1991
ANSI T1.105	Telecommunications - Digital Hierarchy - Optical Interface Rates and Formats Specifications, 1991
ANSI T1.106	Telecommunications - Digital Hierarchy - Optical Interface Specifications, 1988
ANSI T1.107	Telecommunications - Digital Hierarchy - Formats Specifications, 1988
ANSI T1.107a	Telecommunications - Digital Hierarchy - Format Specifications (DS3 Format Applications), 1990
ANSI T1.107b	Telecommunications - Digital Hierarchy - Format Specifications (Synchronous Digital Data Formats), 1991
ANSI T1.109	Telecommunications - Exchange-Interexchange Carrier Interfaces - 950+XXXX EC-to-IC Access Signaling Protocols, 1990
ANSI T1.110	Telecommunications - Signaling System No. 7 (SS7) - General Information, 1992
ANSI T1.111	Telecommunications - Signaling System Number 7 - Functional Description of the Signaling System Message Transfer Part (MPT), 1992
ANSI T1.112	Telecommunications - Signaling System Number 7 - Signaling Connection Control Part (SCCP), 1992
ANSI T1.113	Telecommunications - Signaling System No. 7 (SS7) - Integrated Services Digital Network (ISDN) User Part, 1992
ANSI T1.113a	Telecommunications - Signaling System No. 7 (SS7) - Integrated Services Digital Network (ISDN) User Part (NxDS0 Multi-Rate Connection), 1993
ANSI T1.114	Telecommunications - Signaling System Number 7 (SS7) - Transaction Capability Application Part (TCAP), 1992
ANSI T1.115	Telecommunications - Monitoring and Measurements for Signaling System Number 7 Networks, 1990
ANSI T1.116	Telecommunications - Signaling System Number 7 (SS7) - Operations, Maintenance and Administration Part (OMAP), 1990

[11] Updated March 1991 from *Accredited Standards Committee X3 - Information Processing Systems Projects Manual*, X3/SD-4, CBEMA, August 1990; *1994 ANSI Catalog;* and periodically, from ASC X3 New Releases.

ANSI T1.117	Telecommunications - Digital Hierarchy - Optical Interface Specifications (Short Reach), 1991
ANSI T1.118	Telecommunications - Signaling System Number 7 (SS7) - Intermediate Signaling Network Identification (ISNI), 1992
ANSI T1.201	Telecommunications - Information Interchange - Structure for the Identification of Location Entities for the North American Telecommunications System, 1987
ANSI T1.202	Telecommunications - Internetwork Operations - Guidelines for Network Management of the Public Switched Networks Under Disaster Conditions, 1988
ANSI T1.203	Telecommunications - Operations and Maintenance - Human-Machine Language, 1988
ANSI T1.204	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Lower-Layer Protocols for Interfaces between Operations Systems and Network Elements, 1992
ANSI T1.205	Telecommunications - Information Interchange - Representation of Places, States of the United States, Provinces and Territories of Canada, Countries of the World, and Other Unique Areas for the North American Telecommunications System, 1988
ANSI T1.206	Telecommunications - Digital Exchanges and PBXs - Digital Circuit Loopback Test Line, 1988
ANSI T1.207	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Terminating Test Line Capabilities and Access Arrangements, 1989
ANSI T1.208	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Upper Layer Protocols for Telecommunications Management Network (TMN) Interfaces between Operations Systems and Network Elements, 1993
ANSI T1.209	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Network Tones and Announcements, 1989
ANSI T1.210	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces, 1993
ANSI T1.210	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Principles of Functions, Architectures, and Protocols for Telecommunications Management Network (TMN) Interfaces, 1993
ANSI T1.211	Information Interchange - Representation of National Security Emergency Preparedness-Telecommunications Service Priority, 1989
ANSI T1.212	Operations, Administration, Maintenance, and Provisioning (OAM&P) - Enhanced Telecommunications Credit Card Physical Characteristics and Numbering Structure, 1990
ANSI T1.213	Coded Identification of Equipment Entities of the North American Telecommunications System for Information Exchange, 1990
ANSI T1.214	Telecommunications - OAM&P - A Generic Network Model for Interfaces between Operations Systems and Network Elements, 1990
ANSI T1.214a	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Generic Network Model for Interfaces between Operations Systems and Network Elements (Managed Object Class Definitions for Performance Monitoring), 1992
ANSI T1.215	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Fault Management Messages for Interfaces between Operations Systems and Network Elements, 1990
ANSI T1.216	Telecommunications - Integrated Services digital Network (ISDN) Management - Basic Rate Physical Layer, 1991
ANSI T1.217	Telecommunications - Integrated Services Digital Network (ISDN) Management - Primary Rate Physical Layer, 1991
ANSI T1.218	Telecommunications - ISDN Management - Data Link and Network Layer, 1991
ANSI T1.219	Telecommunications - ISDN Management - Overview and Principles, 1991
ANSI T1.220	Telecommunications - Information Interchange - Coded Representation of the North American Telecommunication Industry Manufacturers, Suppliers, and Related Service Companies, 1991
ANSI T1.221	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - In-Service, Non-intrusive Measurement Device (INMD) - Voice Service Measurements, 1991
ANSI T1.224	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Protocols for Interfaces between Operations Systems in Different Jurisdictions, 1992
ANSI T1.226	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Management of Functions for Signaling System No. 7 (SS7) Network Interconnections, 1992
ANSI T1.227	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Extension to Generic Network Model for Interfaces between Operations Systems across Jurisdictional Boundaries to Support Fault Management, 1992
ANSI T1.228	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Services for Interfaces between Operation Systems across Jurisdictional Boundaries to Support Fault Management, 1992
ANSI T1.229	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Performance Management Functional Area Services for Interfaces between Operations Systems and Network Elements, 1992
ANSI T1.231	Telecommunications - Digital Hierarchy - Layer 1 In-Service Digital Transmission Performance Monitoring, 1993

ANSI T1.233	Telecommunications - Operations, Administration, Maintenance, and Provisioning (OAM&P) - Security Framework for Telecommunications Management Network (TMN) Interfaces, 1993
ANSI T1.309	Telecommunications - Digital Circuit Multiplication Equipment - Interface Functional and Performance Specification, 1991
ANSI T1.312	Telecommunications - Voice Packetization - Packetized Voice Protocol, 1991
ANSI T1.314	Digital Processing of Video Signals - Video Coder/Decoder for Audiovisual Services at 56 to 1,536 kbit/s, 1991
ANSI T1.401	Telecommunications - Interface between Carriers and Customer Installations - Analog Voice-grade Switched Access Lines Using Loop-Start and Ground-Start Signaling, 1993
ANSI T1.403	Integrated Services Digital Network - Carrier-to-Customer Installation - DS1 Metallic Interface, 1989
ANSI T1.404	Telecommunications - Carrier-tc-Customer Installation - DS3 Metallic Interface Specification, 1989
ANSI T1.405	Telecommunications - Interface between Carriers and Customer Installations - Analog Voice-grade Switched Access Using Loop Reverse Battery Signaling, 1989
ANSI T1.407	Telecommunications - Interface between Carriers and Customer Installations - Analog Voice-grade Special Access Lines Using Customer Installation Provided Loop-Start Supervision, 1990
ANSI T1.408	Telecommunications - ISDN Primary Rate - Customer Installation Metallic Interfaces Layer 1 Specification, 1990
ANSI T1.409	Telecommunications - Interface between Carriers and Customer Installations - Analog Voice-grade Special Access Lines Using E&M Signaling, 1991
ANSI T1.410	Telecommunications - Carrier-to-Customer Metallic Interface - Digital Data at 64 kbit/s and Subrates, 1992
ANSI T1.501	Telecommunications - Network Performance Standards - Tandem Encoding Limits for 32 kbit/s Adaptive Differential Pulse-Code Modulation (ADPCM), 1988
ANSI T1.502	Telecommunications - System M-NTSC Television Signals - Network Interface Specifications and Performance Parameters, 1988
ANSI T1.503	Telecommunications - Network Performance Parameters for Dedicated Digital Services - Definitions and Measurement Methods, 1989
ANSI T1.504	Telecommunications - Packet-Switched Data Communications Service - Performance Parameters, 1989
ANSI T1.504b	Telecommunications - Packet-Switched Data Communications Service - Performance Objective, 1993
ANSI T1.505	Telecommunications - Advanced Digital Program Audio Services - Analog Interface and Performance, 1989
ANSI T1.505a	Telecommunications - Packet-Switched Data Communications Service - Performance Measurement Methods, 1991
ANSI T1.506	Telecommunications - Switched Exchange Access Network Transmission Specifications, 1989
ANSI T1.506a	Telecommunications - Network Performance - Transmission Specifications for Switched Exchange Access Network (Absolute Round-Trip Delay), 1992
ANSI T1.507	Telecommunications - Network Performance - Parameters for Circuit Switched Digital Services - Definitions and Measurements, 1990
ANSI T1.508	Telecommunications - Network Performance - Loss Plan for Evolving Digital Networks, 1992
ANSI T1.508a	Telecommunications - Network Performance - Loss Plan for Evolving Digital Networks, 1993
ANSI T1.601	Integrated Services Digital Network - Basic Access Interface for Use on Metallic Loops for Application on the Network Side of the NT (Layer 1 Specification), 1992
ANSI T1.602	Telecommunications - Integrated Services Digital Network (ISDN) - Data-Link Layer Signaling Specification for Application at the User-Network Interface, 1989
ANSI T1.603	Telecommunications - Minimal Set of Bearer Services for the ISDN Primary Rate Interface, 1990
ANSI T1.604	Telecommunications - Minimal Set of Bearer Services for the ISDN Basic Rate Interface, 1990
ANSI T1.605	Integrated Services Digital Network - Basic Access Interface at S and T Reference Points (Layer 1 Specification), 1991
ANSI T1.606	Telecommunications - Integrated Services Digital Network (ISDN) - Architectural Framework and Service Description for Frame-Relaying Bearer Service, 1990
ANSI T1.606a	Telecommunications - Integrated Services Digital Network (ISDN) - Architectural Framework and Service Description for Frame-Relaying Bearer Service (Congestion Management and Frame Size), 1992
ANSI T1.606b	Telecommunications - Integrated Services Digital Network (ISDN) - Architectural Framework and Service Description for Frame-Relaying Bearer Service (Network-to-Network Interface Requirements), 1993
ANSI T1.607	Telecommunications - Integrated Services Digital Network (ISDN) - Layer 3 Signaling Specification for Circuit-Switched Bearer Service for Digital Subscriber Signaling System Number 1, 1990
ANSI T1.608	Telecommunications - Integrated Services Digital Network (ISDN) - Signaling Specification for X.25 Packet-Switched Bearer Service for Digital Subscriber Signaling System Number 1, 1991

ANSI T1.609	Telecommunications - Interworking between the ISDN User-Network Interwork Interface Protocol and the Signaling System Number 7 ISDN User Part, 1990
ANSI T1.610	Telecommunications - Digital Subscriber Signaling System No. 1 (DSS1) - Generic Procedures for the Control of ISDN Supplementary Services, 1990
ANSI T1.610a	Telecommunications - Digital Subscriber Signaling System No. 1 (DSS1) - Generic Procedures for the Control of ISDN Supplementary Services (Display Procedures), 1992
ANSI T1.611	Telecommunications - Signaling System Number 7 (SS7) - Supplementary Services for non-ISDN Subscribers, 1991
ANSI T1.612	Telecommunications - Integrated Services Digital Network (ISDN) - Terminal Adaption Using Statistical Multiplexing, 1992
ANSI T1.613	Telecommunications - Digital Subscriber Signaling System No. 1 (DSS1) ISDN Call Waiting, 1991
ANSI T1.614	Telecommunications - Packet-Mode Bearer Service Category Description, 1991
ANSI T1.615	Telecommunications - Digital Subscriber Signaling System No. 1 (DSS1) - Layer 3 Overview, 1992
ANSI T1.616	Telecommunications - Integrated Services Digital Network (ISDN) - Call Hold Supplementary Services, 1992
ANSI T1.617	Integrated Services Digital Network - DSS1 - Signaling Specification for Frame Relay Bearer Service, 1991
ANSI T1.618	Integrated Services Digital Network - Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service for Digital Subscribers Signaling System Number 1 (DSS1), 1991
ANSI T1.619	Telecommunications - Integrated Services Digital Network (ISDN) - Multi-Level Precedence and Presumption (MLPP) Service Capability, 1991
ANSI T1.620	Telecommunications - Integrated Services Digital Network (ISDN) - Circuit-Mode Bearer Service Category Description, 1991
ANSI T1.621	Telecommunications - Integrated Services Digital Network (ISDN) - User-to-User Signaling Supplementary Service, 1992
ANSI T1.623	Telecommunications - Digital Subscriber Signaling System Number 1 (DSS1) - Signaling Specification for the User Signaling Bearer Service, 1993
ANSI T1.624	Telecommunications - Broadband ISDN User-Network Interfaces - Rates and Formats Specifications, 1993
ANSI T1.625	Telecommunications - Integrated Services Digital Network (ISDN) - Calling Line Identification Presentation and Restriction Supplementary Services, 1993
ANSI T1.626	Telecommunications - Switched-Computer Applications Interface (SCAI), 1993
ANSI T1.627	Telecommunications - Broadband ISDN - ATM Layer Functionality and Specification, 1993
ANSI T1.628	Telecommunications - Routing, Bridging, and Transfer of Emergency Service Calls (RBTESC), 1993
ANSI T1.629	Telecommunications - Broadband ISDN - ATM Adaptation Layer 3/4 Common Part Functions and Specification, 1993
ANSI T1.630	Telecommunications - Broadband ISDN - ATM Adaptation Layer for Constant Bit Rate Services Functionality and Specification, 1993
ANSI T1.631	Telecommunications - Signaling System No. 7 (SS7) - High Probability of Completion (HPC) Network Capability, 1993
ANSI X3/TR-7-89	Information Processing Systems Technical Report - User Documentation for Consumer Software Packages, 1989
ANSI X3/TR-8-89	Information Processing Systems Technical Report - Real-Time Extensions for PL/1, 1989
ANSI X3/TR-11-92	Information Processing Systems Technical Report - IRDS Support for Naming Convention Validation (NCV), 1992
ANSI X3/TR-12-93	Information Processing Systems Technical Report - Repository Context Information Resource Dictionary System (IRDS) Reference Model, 1993
ANSI X3.1	Information Systems - Data Transmission - Synchronous Signalling Rates, 1987 (Reaffirmed in 1992) (FIPS 22-1)
ANSI X3.4	Coded Character Sets - 7-Bit American National Standard Code for Information Exchange (7-Bit ASCII), 1986 (Reaffirmed in 1992) [ISO 646]
ANSI X3.9	Programming Language FORTRAN, 1978 (Reaffirmed in 1989) (ISO 1539)
ANSI X3.15	Bit Sequencing of the American National Standard Code for Information Exchange in Serial-By-Bit Data Transmission, 197 (Reaffirmed in 1990) (FIPS 16-1; ISO 1177] (revision in process)
ANSI X3.23	Programming Language COBOL, 1985 (Reaffirmed in 1991) (ISO 1989)
ANSI X3.23a	Programming Language Intrinsic Function Module for COBOL, 1989 (Reaffirmed in 1991)
ANSI X3.23b-199x	Correction Amendment to American National Standard COBOL ANSI X3.23-1985[R1991] and ANSI X3.23A-1989 [R1991]
ANSI X3.28	Procedures for the Use of the Communications Control Characters of American National Standard Code for Information Interchange (ASCII) in Specified Data Communication Links, 1976 (Reaffirmed in 1992)
ANSI X3.32	Graphic Representation of the Control Characters of American Standard Code for Information Interchange (ASCII), [ISO 2047-75], Revised 1990

ANSI X3.41	Code Extension Techniques for Use with the 7-Bit Coded Character Set of American National Standard Code for Information Interchange (ASCII), 1974, Revised 1990 (FIPS 35, Withdrawn; ISO 2022-82])
ANSI X3.42	Representation of Numeric Values in Character Strings for Information Interchange, [ISO 6093.2], 1975, Revised 1990
ANSI X3.44	Determination of the Performance of Data Communications Systems, 1990
ANSI X3.53	Programming Language PL/1, 1976 (Reaffirmed in 1993) (ISO 6160)
ANSI X3.57	Structure for Formatting Message Headings for Information Interchange Using the American National Standard for Information Interchange (ASCII) for Data Communication System Control, 1977 (Reaffirmed in 1991)
ANSI X3.60	Programming Language Minimal BASIC, Draft (DP 6373]
ANSI X3.61	Representation of Geographic Point Locations for Information Interchange, 1986 (Reaffirmed in 1992)
ANSI X3.66	Advanced Data Communication Control Procedures (ADCCP), 1979 (Reaffirmed in 1992) (FIPS 71)
ANSI X3.74	Information Systems - Programming Language - PL/1 General Purpose Subset, 1987 (Reaffirmed in 1992) (DP 6522)
ANSI X3.79	Determination of Performance of Data Communications Systems that Use Bit Oriented Communications Control Procedures, 1981 (Reaffirmed in 1992)
ANSI X3.83	Information System - ISO Registration According to ISO 2375, ANSI Sponsorship Procedures, 1989 [ISO 2375]
ANSI X3.88	Computer Program Abstracts, 1981 (Reaffirmed in 1992)
ANSI X3.91M	Information Systems - Storage Module Interfaces, 1987 (Reaffirmed in 1992)
ANSI X3.92	Data Encryption Algorithm, 1981 (Reaffirmed in 1987)
ANSI X3.97	Programming Language Pascal, 1983 (DIS 7185)
ANSI X3.98	Text Information Interchange in Page Image Format (PIF), 1983
ANSI X3.100	Information Systems - Interface between DTE and DCE for Operation with Packet-Switched Data Communications Networks (PSDN), or Between Two DTEs, by Dedicated Circuit, 1989
ANSI X3.100a	Information Systems - Interface between DTE and DCE for Operation with Packet-Switched Data Communications Networks (PSDN), or Between Two DTEs, by Dedicated Circuit (NUI and NUI-Derived Extensions), 1991
ANSI X3.102	Data Communication Systems and Services - User-Oriented Performance Parameters, 1992
ANSI X3.105	Information Systems - Data Link Encryption, 1983 (Reaffirmed in 1990)
ANSI X3.106	Information Systems - Data Encryption Algorithm - Modes of Operation, 1983 (Reaffirmed in 1990)
ANSI X3.107	Data Link Layer Protocol for Local Distributed Data Interfaces (LDDI), August 1982 (DP)
ANSI X3.108	Information Systems - Local Distributed Data Interfaces (LDDI) - Physical Layer Interface to Nonbranching Coaxial Cable Bus, 1988
ANSI X3.109	Physical Layer Protocol for Local Distributed Data Interfaces (LDDI), 1982 (DP)
ANSI X3.110	Videotex/Teletext Presentation Level Protocol (North American PLPS), 1983 (Reaffirmed in 1991) (FIPS 121) [ISO 6937/1-2]
ANSI X3.113	Information Systems - Programming Languages - Full BASIC, 1987 (Reaffirmed in 1993) (FIPS 68-2) [DP 10279]
ANSI X3.113a	Information Systems - Programming Languages - Modules and Individual Character Input for Full BASIC, 1989 (Reaffirmed in 1993) (FIPS 68-2)
ANSI X3.122	Computer Graphics Metafile (CGM) for the Storage and Transfer of Picture Description Information, 1986 (withdrawn and replaced by ISO 8632:1990, Parts 1-4)
ANSI X3.122.5	LISP Binding of GKS, Draft, 1989
ANSI X3.123	Programming Language APL, Draft, 1989 (DP 8485)
ANSI X3.124	Computer Graphics - Graphical Kernel System (GKS) Functional Description, 1985 (Reaffirmed in 1991) (ISO 7942)
ANSI X3.124.1	Information Systems - Computer Graphics - Graphical Kernel System (GKS) FORTRAN Language Binding, 1985 (Reaffirmed in 1993) (ISO 8651-1)
ANSI X3.124.2	Computer Graphics - Graphical Kernel System (GKS) Pascal Language Binding, 1988 (ISO 8651-2)
ANSI X3.124.3	Computer Graphics - Graphical Kernel System (GKS) Ada Language Binding, 1989 (ISO 8651-3)
ANSI X3.124.4	Computer Graphics - Graphical Kernel System (GKS) C Binding, Draft, 1989 (DP 8651-4)
ANSI X3.129	Intelligent Peripheral Interface, Physical Level, 1986 (Reaffirmed in 1992) [ISO 9318-1]
ANSI X3.130	Intelligent Peripheral Interface - Device-Specific Command Set for Magnetic Disks, 1986 [ISO 9318-2]
ANSI X3.131	Small Computer System Interface (SCSI), 1986 [ISO 9316]
ANSI X3.132	Information Systems - Intelligent Peripheral Interface - Device Generic Command Set for Magnetic and Optical Disks, 1987 [ISO 8907] (withdrawn and replaced by ANSI/ISO 9318-3-1990)
ANSI X3.133	Database Language - NDL, 1986 (Reaffirmed in 1992) (FIPS 126)
ANSI X3.134.1	8-Bit ASCII Structure and Rules, Draft
ANSI X3.134.2	7-Bit and 8-Bit ASCII Supplemental Multilingual Graphic Character Set (ASCII Multilingual Set), Draft

ANSI X3.135	Information Systems - Database Language - SQL, 1992 (FIPS 127-1) (ISO 9075:1992)
ANSI X3.138	Information Systems - Information Resource Dictionary System (IRDS), 1988 (DIS 10027) (FIPS 156)
ANSI X3.138a	Information Systems - Information Resource Dictionary System (IRDS) (Supplement to X3.138-1988), 1991
ANSI X3.139	Information Systems - Fiber Distributed Data Interface (FDDI) - Token Ring Media Access Control (MAC), 1987 (Reaffirmed in 1992) [DP 9314-2]
ANSI X3.140	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Layer Protocol Specification, 1986 (withdrawn and replaced by ANSI/ISO 8072-1986 and ANSI/ISO 8073-1991)
ANSI X3.141	Information Systems - Data Communication Systems and Services - Measurement Methods for User-Oriented Performance Evaluation, 1987 (Reaffirmed in 1992)
ANSI X3.143	Information Processing Systems - Text and Office Systems - Standard Generalized Markup Language (SGML), Draft [ISO 8879]
ANSI X3.144	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Functional Description, 1988 (withdrawn and replaced by ANSI/ISO 9592-1989, Parts 1-3)
ANSI X3.144.1	FORTRAN Language Binding of the Programmer's Hierarchical Interactive Graphics System (PHIGS), 1988 (withdrawn and replaced by ANSI/ISO 9593-1-1992)
ANSI X3.144.2	Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Binding to Pascal, Draft, 1987 (DIS 9593-2)
ANSI X3.144.3	Information Processing Systems - Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) Binding to Ada, 1988 (withdrawn and replaced by ANSI/ISO 9593-3-1992)
ANSI X3.144.4	Computer Graphics - Programmer's Hierarchical Interactive Graphics System (PHIGS) C Language Binding, Draft, 1991 (ISO 9593-4)
ANSI X3.146	Information Systems - Streaming Cartridge and Cassette Tape Drives - Device-Level Interface, 1986
ANSI X3.147	Intelligent Peripheral Interface - Device Generic Command Set for Magnetic Tape, 1987 [ISO 9318-4] (not listed in *1994 ANSI Catalog*)
ANSI X3.148	Information Systems - Fiber Distributed Data Interface (FDDI) - Physical Layer Protocol (PHY), 1988 (ISO 9314-1)
ANSI X3.153	Information Systems - Open Systems Interconnection - Basic Connection Oriented Session Protocol Specification, 1987 (withdrawn and replaced by ANSI/ISO 8326-1987 and 8327-1987)
ANSI X3.159	Information Systems - Programming Languages - Programming Language C, 1989 (ISO 9899: 1990; FIPS-160) (withdrawn and replaced by ANSI/ISO 9899-1990)
ANSI X3.160	Programming Language Extended Pascal, 1990 [replaced by ANSI/IEEE 770 X3.160-1989]
ANSI X3.161	Computer Graphics Interface (CGI), 1990 [replaced by ISO 9636)
ANSI X3.165	Information Systems - Programming Language - DIBOL (revision of ANSI X3.165-1988), 1992
ANSI X3.166	Fiber Distributed Data Interface (FDDI) - Physical Layer Medium Dependent (PMD), 1990 [ISO 9314-3]
ANSI X3.167	Local Distributed Data Interface (LDDI) Star-Wired Physical Interface Sublayer, Draft, 1987 (DP)
ANSI X3.168	Information Systems - Database Language- Embedded SQL (withdrawn; now included in ANSI X3.135-1992)
ANSI X3.170	Information Systems - Data Communication - Enhanced Small Device Interface (ESDI), 1990 [DIS 10222]
ANSI X3.170a	Information Systems - Data Communication - Enhanced Small Device Interface (ESDI), 1991 (enhancement to ANSI X3.170-1990)
ANSI X3.172	American National Standard Dictionary for Information Systems (ANDIS), 1990 (now includes X3.172a-1992)
ANSI X3.172a	Information Systems - Dictionary for Information Systems (Computer Security Glossary), 1992
ANSI X3.172x	Hypermedia and Multimedia Glossary, X3K5, new project
ANSI X3.176	Intelligent Peripheral Interface Device - Specific Command Set for Magnetic Tapes, 1990, [ISO 9318-5]
ANSI X3.177	Intelligent Peripheral Interface, Device - Generic Command Set for Communications, 1990, [ISO 9318-7]
ANSI X3.178	Information Systems - Packet-switched Signalling System Between Public Networks Providing Data Transmission Service, 1990
ANSI X3.178a	Information Systems - Packet-switched Signalling System Between Public Networks Providing Data Transmission Service (NUI Utility Extensions and Format Constraints), 1991
ANSI X3.183	Information Systems - High-Performance Parallel Interface (HPPI), 1991
ANSI X3.184	Information Systems - Fiber Distributed Data Interface (FDDI) - Single Mode Physical Layer Medium Dependent (SMF-PMD) (CD 9314-4), 1993
ANSI X3.185	Information Systems - Information Resource Dictionary Systems - IRDS Services Interface, 1992
ANSI X3.186	Information Systems - Fiber Distributed Data Interface (FDDI) - Hybrid Ring Control (HRC), 1992

ANSI X3.189	Information Systems - Interface Between DTE and DCE for Terminals Operating in the Packet Mode and Accessing a Packet-Switched Public Data Network Through Switched Access, 1991
ANSI X3.190	Information Technology - Text and Office Systems - Conformance Testing for SGML Systems, 1992
ANSI X3.195	Information Systems - Information Resource Dictionary System (IRDS) - Export/Import File Format, 1991
ANSI X3.196	Computer Graphics - X Window System Data Stream Definition, Draft
ANSI X3.198	Programming Language - FORTRAN - Extended, 1992
ANSI X3.201	Information Systems - Intelligent Peripheral Interface (IPI) - Enhanced Physical Level, 1992
ANSI X3.209	Information Systems - Optical Character Recognition (OCR) - Matrix Character Sets for OCR-MB, 1991
ANSI X3.210	Information Systems - High-Performance Parallel Interface - Framing Protocol (HPPI-FP), 1992
ANSI X3.215	Programming Language FORTH, DRAFT
ANSI X3.216	Information Processing Systems - Data Communications - Structure and Semantics of the Domain Specific Part (DSP) of the OSI Network Service Access Point (NSAP) Address, 1992
ANSI X3.218	Information Systems - High-Performance Parallel Interface (HPPI) - Encapsulation of ISO 8802-2 (IEEE Std 802.2) Logical Link Control Protocol Data Units (HPPI-LE), 1993
ANSI X3.219	X Window System Data Stream Definition, Part IV: Mapping onto Open Systems Interconnection
ANSI X3.222	Information Systems - High-Performance Parallel Interface (HPPI) - Physical Switch Control (HPPI-SC), 1993
ANSI X3.226	Programming Language Common LISP, Draft
ANSI X3.228	X.25 Data Transfer Phase (DTP) Procedures for Operation with Frame Relay, 1993
ANSI X3.229-199x	FDDI, Part 6: Station Management (SMT) Standard, Revision 7.2
ANSI X3.238	Programming Language DATABUS, Draft
ANSI X3H4.6	Technical Report on Model Unification for Data Repositories
ANSI X3S3.7	X.25 Data Transfer Phase Procedures for Operating the Packet Layer Transfer Phase of X.25
ANSI X3T9.5	FDDI Follow-On Local Area Network - Physical Medium Dependent (FFOL-PMD), new project, 10 May 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Physical Layer Protocol (FFOL-PHY), new project, 10 May 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Service Multiplexer (FFOL-SMUX), new project, 10 May 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Asynchronous Media Access Control (FFOL-AMAC), new project, May 10, 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Isochronous Media Access Control (FFOL-IMAC), new project, May 10, 1991
ANSI X3T9.5	FDDI Follow-On Local Area Network - Station Management (FFOL-SMT), new project, 10 May 1991
ANSI X3V1.4	Voice Messaging over MOTIS ISO/DIS 10021
ANSI X3V1.9	Standard User Interface to Voice Messaging
ANSI X3 682-D	Domestic Public/Private X.25 Network Interworking, Draft
ANSI X9.30	Public Key Cryptography, Part 2, 1993
ANSI X12 Series	Electronic Data Interchange (ISO 9735) (Parts 1 to 50), 1992
ANSI Y14.26M	Digital Representation for Communication of Product Definition Data, Draft, 1989
ANSI Z.39.50-1992	Information Retrieval - Application Service Definition and Protocol Specification for Open Systems Interconnection, 1992 (renamed ANSI/NISO Z39.50-1992)
ANSI Z.39.50-MA-026	Implementors Group Profile
EIA-232C	Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange, Third Edition (also known as RS-232C)
EIA-232D	Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Binary Data Interchange, Fourth Edition (also known as RS-232D)
FED-STD 1041	Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DTE) for Operation with Pack-Switched Data Communications Network, National Communications System
HFS/ANSI 100-1988	Human Factors Engineering of Video Display Terminal Workstation Standard, 1988
IEEE 610	IEEE Standard Computer Dictionary Compilation of IEEE Standard Computer Glossaries, 1990
IEEE 610.2	IEEE Standard Glossary Computer Applications Terminology, 1987
IEEE 610.3	IEEE Standard Glossary of Modeling and Simulation Terminology, 1989
IEEE 610.4	IEEE Standard Glossary of Image Processing and Pattern Recognition Terminology, 1990
IEEE 610.5	IEEE Standard Glossary of Data Management Terminology, 1990

IEEE 610.6	IEEE Standard Glossary of Computer Graphics Terminology, 1991
IEEE 610.12	IEEE Standard Glossary of Software Engineering Terminology , 1990
IEEE 610.12A	IEEE Standard Glossary of Software Engineering Terminology - ASCII Version, 3 1/2-inch Diskette with Soft bound Text, 1990
IEEE 610.12B	IEEE Standard Glossary of Software Engineering Terminology - ASCII Version, 5 1/4-inch Diskettes with Soft bound Text, 1990
IEEE 610.12H	IEEE Standard Glossary of Software Engineering Terminology - HyperCard Stack, diskette only (HyperCard v.1.2 and up),1990
IEEE 610.13	IEEE Standard Glossary of Computer Languages, 1993
IEEE 660	IEEE Standard for Semiconductor Memory Test Pattern Language, 1986, reaffirmed 1991
IEEE 662	IEEE Standard Terminology for Semiconductor Memory, 1980
IEEE 696	IEEE Standard 696 Interface Devices, 1983, reaffirmed 1991
ANSI/IEEE 729	IEEE Standard Glossary of Software Engineering Terminology, 1983
ANSI/IEEE 730	IEEE Standard for Software Quality Assurance Plans, 1989
IEEE 754	IEEE Standard for Binary Floating-Point Arithmetic, 1985, reaffirmed 1991
IEEE 770	Programming Language Pascal, 1990
IEEE 796	IEEE Standard Microcomputer System Bus, 1983 (reaffirmed 1988)
IEEE 802	IEEE Standards for Local and Metropolitan Area Networks: Overview and Architecture, 1990
IEEE 802.1B	IEEE Standards for Local and Metropolitan Area Networks: LAN/MAN Management, 1992
IEEE 802.1D-1993	Information Technology - Telecommunications and Information Exchange Between Systems - Local Area Networks - Media Access Control (MAC) Bridges (same as ISO/IEC 10038:1993)
IEEE 802.1E	IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Layer Management (Section 5). 1990
IEEE 802.1i	IEEE Supplement to Media Access Control (MAC) Bridges: Fiber Distributed Data Interface (FDDI), 1992
IEEE 802.1k	LAN/MAN (Local Area Network/Metropolitan Area Network) Management: Standard for Discovery and Dynamic Control of Event Forwarding (supplement to 802.1B), 1993
IEEE 802.1m	Standard for System Load Protocol Supplement: Managed Object Definitions and Protocol Implementation Conformance Statement (PICS) Proforma (supplement to 802.1E), 1993
IEEE 802.3-1993	Information Technology - Local and Metropolitan Area Networks - Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (same as ISO/IEC 8802-3:1993)
IEEE 802.3h	IEEE Standards for Local and Metropolitan Area Networks: System Load Protocol, 1990
IEEE 802.3i	IEEE Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: System Considerations for Multisegment 10 Mb/s Baseband Networks (Section 13) and Twisted-Pair Medium Attachment Unit (MAU) and Baseband Medium, Type 10BASE-T (Section 14), 1990
IEEE 802.3k	IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Layer Management for 10 Mb/s Baseband Repeaters (Section 19), 1992
IEEE 802.3l	IEEE Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications: Type 10BASE-T MAU Protocol Implementation Conformance Statement (PICS) Proforma, 1992
IEEE 802.3p	Standard for Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method: Layer Management for 10 Mb/s Baseband Medium Attachment Units (MAUs), 1993
IEEE 802.3q	Standard for Carrier Sense Multiple Access with Collision Detection (CSMA/CE) Access Method: Guidelines for the Development of Managed Objects (GDMO) (ISO 10164-4) Format for Layer Managed Objects, 1993
IEEE 802.4b	IEEE Supplement to Token-Passing Bus Access Method and Physical Layer Specifications: Enhancements for Physical Layer Diversity, 1992
IEEE 802.5c	IEEE Supplement to Token-Passing Bus Access Method and Physical Layer Specifications: Recommended Practice for Dual Ring Operation with Wrapback Reconfiguration, 1991
IEEE 802.5m	Supplement to ISO/IEC 10038:1993, Source Routing, 1993
IEEE P802.5q	Standard for Information Technology-Local and Metropolitan Area Networks-Part 5: Token Ring Access Method and Physical Layer Specification- Media Access Control Revision
IEEE 802.6	IEEE Standards for Local and Metropolitan Area Networks: Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network (MAN), 1990
IEEE 802.6c	Standard for DS1 Physical layer Convergence Procedures for 802.6 MAN, 1993
IEEE 802.6d	Standard for SONET (SDH) Based Physical Layer convergence Procedures for 802.6 MAN, 1993
IEEE 802.6f	Standard for Conformance Statement for the 802.6 Base Standard, 1993
IEEE 802.6k	Supplement to Media Access Control (MAC) Bridges: IEEE Standard 802.6 Distributed Queue Dual Bus Subnetwork of Metropolitan Area Network (MAN), 1992
IEEE 802.7	IEEE Recommended Practices for Broad band Local Area Networks, 1989
IEEE P802.10A	Interoperable LAN Security (SILS) - The Model [PAR approved 5/90]

IEEE 802.10B	IEEE Standards for Local and Metropolitan Area Networks: Standard for Interoperable LAN Security (SILS), Part B: Secure Data Exchange, 1992
IEEE P802.10C	SILS - Key Management [PAR approved 5/90]
IEEE P802.10D	SILS - Security Management [PAR approved 5/90]
IEEE P802.11	Standard for Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications [PAR approved March 21, 1991]
IEEE 828	Standard for Software Configuration Management Plans, 1990
ANSI/IEEE 829	IEEE Standard for Software Test Documentation, 1983 (Standard reaffirmed March 21, 1991])
ANSI/IEEE 830	IEEE Guide to Software Requirements Specifications, 1984 (Revision underway)
IEEE 896.2-1991	Futurebus+, Physical Layer and Profile Specifications, 1993
IEEE 896.3	Recommended Practices for Futurebus+, 1993
IEEE 896.5	Standard for Futurebus+, Profile M (Military), 1993
IEEE 982.1	IEEE Standard Dictionary of Measures to Produce Reliable Software, 1988
IEEE 982.2	IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software, 1988
ANSI/IEEE 983	IEEE Guide for Software Quality Assurance Planning, 1986
ANSI/IEEE 990	IEEE Recommended Practice for Ada as a Program Design Language, 1986
ANSI/IEEE 1002	IEEE Standard Taxonomy for Software Engineering Standards, 1987, REAFFIRMED 1992
IEEE 1003	IEEE Standard Interpretations: IEEE Standard Portable Operating System Interface for Computer Environments, 1988
IEEE P1003.0	POSIX Guide, Draft 15, balloted July 1992
IEEE 1003.1	POSIX, approved as IEEE Std. 1003.1-1988 and revised September 1990
IEEE P1003.1	Language Independent Specifications, as IEEE Std. 1003.1-1990, ISO 9945-1 and FIPS 152-2, Draft 3, May 1992
IEEE P1003.1/LIS	See IEEE P1372
IEEE P1003.1a	System API Extensions, Draft 7, balloted late 1992
IEEE 1003.1b	Real-Time Extensions, Draft 13x recirculated, October 1992 (formerly IEEE 1003.4)
IEEE 1003.1c	Threads, Draft 7 recirculated May 1992 (formerly IEEE P1003.4a)
IEEE 1003.1d	Extensions to .4, Draft 5, September 1992, 1st ballot, 1Q 1993 (formerly IEEE P1003.4b)
IEEE P1003.1e	System API Security Addendum (formerly IEEE P1003.6.1)
IEEE P1003.1f	Transparent File Access (TFA), Draft 6, 2Q 1992 (formerly IEEE P1003.8)
IEEE 1003.1g	Protocol Independent Network Interfaces, Draft 1.4, balloting planned for 2Q 1993 (formerly IEEE P1003.12)
IEEE 1003.2	Shell and Utilities, approved September 7, 1992
IEEE 1003.2a	User Portability Interfaces, approved as part of IEEE Std. 1003.2
IEEE P1003.2c	Shell and Utility Security Addendum (formerly IEEE P1003.6.2)
IEEE P1003.2d	POSIX, Part 2: Shell and Utilities - Amendment: Batch Environment (PAR approved) (formerly IEEE P1003.15a)
IEEE 1003.3	Test Methods, IEEE 1003.3-1991 approved March 21, 1991. ISO standard proposed; international ballot initiation pending (see IEEE 2003)
IEEE 1003.3.1	Test Methods for POSIX.1, approved December 1992 (see IEEE 2003.1)
IEEE P1003.3.2	Test Methods for Measuring Conformance to POSIX, Draft 8 balloted 4Q 1992 (see IEEE 2003.2)
IEEE 1003.4	Real-Time Extensions, Draft 13x recirculated, October 1992 (see IEEE 1003.1b)
IEEE P1003.4a	Threads, Draft 7 recirculated May 1992 (see IEEE 1003.1c)
IEEE P1003.4b	Extensions to .4, Draft 5, September 1992, 1st ballot, 1Q 1993 (see IEEE 1003.1d)
IEEE 1003.5	POSIX Ada Language Binding, approved June 1992, [PAR approved for revision October 1993. The new title will be POSIX Ada Language Interfaces - Part 1: Binding for System Application Program Interface (API)]
IEEE P1003.5b	Ada Language (Real Time) Bindings; ballot planned for December 1993 (formerly IEEE P1003.20)
IEEE P1003.6	Security Extensions, Draft 12, October 1991 (see IEEE P1003.1e and IEEE P1003.2c)
IEEE P1003.6.1	System API Security Addendum
IEEE P1003.6.2	Shell and Utility Security Addendum
IEEE P1003.7	Administered Systems (name changed from System Administration Interface), Work is being "sliced" into ballotable partitions which will be balloted separately in 1Q 1993 (see IEEE P1387)
IEEE P1003.7.1	Amendment 1: Print Administration, [PAR approved, March 19, 1992], Draft (see IEEE P1387.4)
IEEE P1003.7.2	Amendment 2: Software Administration [PAR approved, March 19, 1992], ballot May 1992 (see IEEE P1387.2)
IEEE P1003.7.3	Amendment 3: User Administration [PAR approved October 1993] (see IEEE P1387.3)
IEEE P1003.8	Transparent File Access (TFA), Draft 6, 2Q 1992 (see IEEE P1003.1f)
IEEE 1003.9	FORTRAN 77 Language Binding, Draft 11 approved June 1992
IEEE P1003.10	Supercomputing Application Environment Profile (AEP), Draft 11, September 1992
IEEE P1003.11	POSIX Based Transaction Processing Applications Environment Profile, PAR approved 1993 (withdrawn)
IEEE P1003.12	Protocol Independent Network Interfaces, Draft 1.4, balloting planned for 2Q 1993 (see IEEE P1003.1g)

IEEE P1003.13	Real-Time AEP, Draft 5, April 1992, ballot May 1992
IEEE P1003.14	Multiprocessing AEP, Draft 5, 7 April 1992
IEEE P1003.15	POSIX Batch Environment Amendments, balloting of Draft 10, November 1992 (to be revised)
IEEE P1003.15a	POSIX, Part 2: Shell and Utilities - Amendment: Batch Environment (PAR approved) (see IEEE P1003.2d)
IEEE P1003.16	C Binding for POSIX.1, Draft 2, May 1992, ballot closed 18 September 1992 [PAR withdrawn October 1991]
IEEE P1003.16a	Amendment 1: System API Extensions [PAR approved, March 19, 1992] [PAR withdrawn October 1991]
IEEE 1003.17	Directory Services API, Draft 4, approved March 1993 (see IEEE P1224.2)
IEEE P1003.18	POSIX Platform Profile, Draft 6, May 1992, balloted 4Q 1992
IEEE P1003.19	POSIX FORTRAN 90 Language Binding, initiated July 1992 [PAR withdrawn October 1991]
IEEE P1003.20	Ada Language (Real Time) Bindings; ballot planned for December 1993 (see IEEE P1003.5b)
IEEE P1003.21	POSIX, Part 1: System Application Programming Interface (API) - Amendment: Real-Time Distributed Systems Communications (PAR approved)
IEEE P1003.22	Guide to the POSIX Open Systems Environment - A Security Framework (PAR approved)
IEEE 1224	OSI Abstract Data Maniuplation API (LIS), 1993
IEEE 1224.2	Directory Services Application Programming Interface (API) - Language Independent Specification approved March 1993 (formerly IEEE P1003.17)
IEEE P1372	Language Independent Specifications, as IEEE Std. 1003.1-1990, ISO 9945-1 and FIPS 152-2, Draft 3, May 1992 (formerly IEEE P1003.1/LIS)
IEEE P1387	Administered Systems (name changed from System Administration Interface); work is being "sliced" into ballotable partitions which will be balloted separately in 1Q 1993 (formerly IEEE P1003.7)
IEEE P1387.2	Amendment 2: Software Administration [PAR approved, March 19, 1992], ballot May 1992 (formerly IEEE P1003.7.2)
IEEE P1387.3	Amendment 3: User Administration [PAR approved October 1993] (formerly IEEE P1003.7.3)
IEEE P1387.4	Amendment 1: Print Administration, [PAR approved, March 19, 1992], Draft 5 mock ballot, 2Q 1992 (formerly IEEE P1003.7.1)
IEEE 2003	Test Methods, IEEE 1003.3-1991 approved March 21, 1991. ISO standard proposed; international ballot initiation pending (formerly IEEE 1003.3)
IEEE 2003.1	Test Methods for Measuring Conformance to POSIX - Part 1: System Interfaces, approved December 1992 (formerly IEEE 1003.3.1)
IEEE 2003.2	Test Methods for Measuring Conformance to POSIX, Draft 8 balloted 4Q 1992 (formerly IEEE 1003.3.2)
ANSI/IEEE 1008	IEEE Standard for Software Unit Testing, 1987
ANSI/IEEE 1012	IEEE Standard for Software Verification and Validation Plans, 1987 [PAR approved for Standard Revision, March 19, 1992]
ANSI/IEEE 1016	IEEE Recommended Practice for Software Design Descriptions, 1987
IEEE 1016.1	IEEE Guide to Software Design Descriptions, 1993
IEEE 1028	IEEE Standard for Software Reviews and Audits, 1988
ANSI/IEEE 1042	IEEE Guide to Software Configuration Management, 1988
IEEE P1044	Standard for Classification of Software Anomalies (formerly entitled Classification of Software Errors/Faults/Failures)
IEEE 1045	Software Productivity Metrics, 1992
ANSI/IEEE 1058.1	IEEE Standard for Software Project Management Plans, 1987 [PAR approved for revision October 1993]
IEEE P1058.2	Guide for Software Project Management Plans [PAR WITHDRAWN March 21, 1991]
IEEE P1059	Software Verification and Validation
IEEE 1061	IEEE Standard for a Software Quality Metrics Methodology, 1992
IEEE P1062	Software Acquisition
ANSI/IEEE 1063	IEEE Standard for Software User Documentation, 1989
IEEE 1074	Standard for Developing Software Life Cycle Processes, (approved September 1991)
IEEE 1076	IEEE Standard VHDL Language Reference Manual, 1987
IEEE 1076 INT.	IEEE Standard VHDL Language Reference Manual Interpretations 1992
IEEE P1076.1	Standard VHDL Language Reference Manual - Analog Extensions, PAR approved July 1993
IEEE P1076.2	Standard VHDL Language Math Package, PAR approved July 1993
IEEE P1076.3	Standard VHDL Language Synthesis Package, PAR approved July 1993
IEEE P1076.4	Standard VHDL Language Timing Methodology, PAR approved July 1993
IEEE P1076.5	Standard VHDL Language Utility Library, PAR approved July 1993
IEEE 1084	IEEE Standard Glossary of Mathematics of Computing Terminology, 1986
IEEE 1154	Standard for Programmed Inquiry Learning, or Tracking, 1991
IEEE 1164	IEEE Standard Multivalue Logic System for VHDL Model Interoperability, 1993
IEEE P1172	Object Oriented Programming Language and Environment, Draft

IEEE 1175	Standard Reference Model for Computing System Tool Interconnections, 1991] [PAR approved for revision October 1993]
IEEE 1178	SCHEME Language Standard, 1990
IEEE P1201.1	Uniform Application Program Interface, Graphical User Interfaces, Draft 3, February 1992
IEEE P1201.2	Driveability Analysis Data, May 1992, ballot closed 17 September 1992
IEEE 1209	Recommended Practice for Evaluation of CASE Tools, 1992
IEEE 1219	Software Maintenance Standard, 1992
IEEE 1224	OSI Abstract Data Manipulation API - Language Independent Specification, 1993
IEEE 1224.1	X.400 Based Electronic Messaging API - Language Independent Specification, 1993
IEEE 1224.2	Directory Services Application Programming Interface (API) - Language Independent Specification, 1993
IEEE P1226.1	Trial use Standard for Common Ada Packages for a Broad Based Environment for Test (ABBET), 1993
IEEE P1228	Software Safety Plans
IEEE P1237	Remote Call Procedure Interface Language, PAR approved May 1990, project moved to X3
IEEE P1238	Common OSI Application Program Interfaces; Draft 4, August 1992, ballot 4Q 1992
IEEE P1238.1	WITHDRAWN
IEEE P1252	Standard for a Frame-based Knowledge Representation, PAR approved July 1993
IEEE P1256	Standard for an Open Basic Input/output System Software (OBIOS), [PAR approved March 21, 1991]
IEEE 1278	IEEE Standard for Information Technology - Protocols for Distributed Interactive Simulation Applications - Entity Information and Interaction, 1993
IEEE P1279	Standard for CD-ROM Architectural Profile [PAR Approved, December 4, 1991]
IEEE P1280	Standard for Information Technology—Data Access Language for Full-Text Information Systems: Structured Full-Text Query Language (SFQL) [PAR approved for standard revision, March 19, 1992]
IEEE P1295.1	Standard for Information Technology—X Window System—Modular Toolkit
IEEE P1295.2	Standard for Information Technology—X Window System—Open Toolkit Environment
IEEE 1298	Software Quality Management System, Part 1: Requirements, 1992
IEEE 1326	Test Methods for Measuring Conformance to OSI Abstract Data Manipulation - API, 1993
IEEE 1326.1	Test Methods for Measuring Conformance to X.400 Based Electronic Messaging Application Program Interfaces (API) [Language Independent], 1993
IEEE 1326.2	Test Methods for Directory Services Application Programming Interface (API) - Language Independent Specification, 1993
IEEE 1327	OSI Abstract Data Manipulation API, 1993
IEEE 1327.1	X.400 Based Electronic Messaging C Language Interfaces - Binding for Applications Program Interfaces (APIs), 1993
IEEE 1327.2	Directory Services Application Programming Interface (API) - C Language Specification, 1993
IEEE 1328	Test Methods for Measuring Conformance to OSI Abstract Data Manipulation C Language Interfaces - Binding for API, 1993
IEEE 1328.1	Test Methods for Measuring Conformance to X.400 Based Electronic Messaging C Language Interfaces - Binding for Applications Program Interfaces (APIs), 1993
IEEE 1328.2	Test Methods for Directory Services Application Programming Interface (API) - C Language Specification, 1993
IEEE P1351	Standard for Information Technology—OSI Application Program Interface—ACSE and Presentation Layer Application Program Interface) Language Independent Specification), PAR approved July 1993
IEEE P1352	Standard for Information Technology—OSI Application Program Interfaces—Test Methods for ACSE and Presentation Layer Application Program Interface (Language-Independent Specification), PAR approved July 1993
IEEE P1353	Standard for Information Technology—OSI Application Program Interfaces—ACSE and Presentation Layer Application Program Interface (C Language Binding), PAR approved July 1993
IEEE P1354	Standard for Information Technology—OSI Application Program Interfaces—Test Methods for ACSE and Presentation Layer Application Program Interface (C Language Binding), PAR approved July 1993
IEEE P1358	Standard for Information Technology—Signal Processing Applications—Processor Graph Method Software Design Methodology, PAR approved July 1993
IEEE P1362	Guide for Information Technology—Systems Definition—Concept of Operation Document, PAR approved July 1993
IEEE P1372	POSIX, Part 1: System Application Program Interface (API) [Language Independent]
IEEE 2003.1	IEEE Standard for Information Technology—Test Methods for Measuring Conformance to POSIX - Part 1: System Interfaces, 1992
NIST	Government Network Management Profile (GNMP), NIST National Computer Systems Laboratory, 3 June 1992
NIST ICT/SNA-85-17	Military Supplement to ISO Transport Protocol, NIST National Computer Systems Laboratory, 1985

NIST ICT/SNA-85-18	Implementation Guide for ISO Transport Protocol, NIST National Computer Systems Laboratory, 1985
NIST SP 500-182	Guidelines for the Evaluation of Message Handling Systems Implementations
NIST SP 500-192	Government Open Systems Interconnection Users Guide, Version 2, NIST, 1992
NIST SP 500-196	Guidelines for the Evaluation of File Transfer, Access and Management Implementations, NIST, 1992
NIST SP 500-205	Guidelines for the Evaluation of Virtual Terminal Implementations, NIST, 1993
NIST SP 500-206	Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 6, Proceedings of the December 1992 NIST OSE Implementor's Workshop (OIW), March 1993
NIST SP-500-210	APP: Application Portability Profile: The U.S. Government's Open System Environment Profile OSE/1 Version 2.0, Systems and Software Technology Division, Computer Systems Laboratory, National Institute of Standards and Technology, June 1993
NIST SP 500-xxx	Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 7, Proceedings of the December 1993 NIST OSE Implementor's Workshop (OIW), January 1994 (electronic edition is available; publication is forthcoming)
NISTIR 4594	GOSIP Conformance and Interoperation Testing and Registration, Version 1, U.S. NIST Systems and Network Architecture (SNA) Division, December 1988
NISTIR 88-4017	Standards for the Interchange of Large Format Tiled Raster Documents, U.S. NIST, December 1988
NIST SP-xxx	Guide on Open System Environment (OSE) Procurements, by Gary E. Fisher, Systems and Software Technology Division, Computer Systems Laboratory, US NIST, DRAFT, November 12, 1993, planned publication date January 1994.
NIST SP 800-4	Computer Security Considerations in Federal Procurements
NIST	Specifications for a Secure Hash Standard, NIST, 22 January 1992 (proposed US FIPS)
FIPS[12] 1-2	Code for Information Interchange, its Representations, Subsets, and Extensions, 14 November 1984, [ANSI X3.4-1977, X3.32-1973 and X3.41-1974]
FIPS 4-1	Representation for Calendar Date and Ordinal Date for Information Interchange, 27 January 1988, [ANSI X3.30-1985(R1991)]
FIPS 5-2	Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas, 28 May 1987
FIPS 6-4	Counties and Equivalent Entities of the United States, its Possessions, and Associated Areas, 31 August 1991, [ANSI X3.21-1988]
FIPS 8-5	Metropolitan Statistical Areas (MSAs), 31 October 1984
FIPS 9-1	Congressional Districts of the United States, 30 November 1990
FIPS 10-3	Countries, Dependencies, Areas of Special Sovereignty, and their Principal Administrative Divisions, 9 February 1984
FIPS 11-3	Guideline: American National Dictionary for Information Systems, 1 February 1991
FIPS 16-1	Bit Sequencing of the Code for Information Interchange in Serial-by-Bit Data Transmission, 1 September 1977, [ANSI X3.15-1976(R1983 & R1990)]
FIPS 17-1	Character Structure and Character Parity Sense for Serial-by-Bit Data Communication in the Code for Information Interchange, 1 September 1977, [ANSI X3.16-1976(R1983 & R1990)]
FIPS 19-1	Catalog of Widely Used Code Sets, 7 January 1985
FIPS 21-3	COBOL, 12 January 1990, [ANSI X3.23-1985 and X3.23A-1989]
FIPS 22-1	Synchronous Signaling Rates Between Data Terminal and Data Communication Equipment, 1 September 1977, [ANSI X3.1-1976]
FIPS 28	Standardization of Data Elements and Representations, 5 December 1973
FIPS 29-2	Interpretation Procedures for Federal Information Processing Standards for Software, 14 September 1987
FIPS 30	Software Summary for Describing Computer Programs and Automated Data Systems, 30 June 1974
FIPS 31	Guidelines for Automatic Data Processing Physical Security and Risk Management, June 1974
FIPS 38	Guidelines for Documentation of Computer Programs and Automated Data Systems, 15 February 1976
FIPS 39	Glossary for Computer Systems Security, 15 February 1976
FIPS 41	Computer Security Guidelines for Implementing the Privacy Act of 1974, 30 May 1975
FIPS 42-1	Guidelines for Benchmarking ADP Systems in the Competitive Procurement Environment, 15 May 1977
FIPS 45	Guide for the Development, Implementation and Maintenance of Standards for the Representation of Computer Processed Data Elements, 30 September 1976
FIPS 46-1	Data Encryption Standard, 22 January 1988 (reaffirmed until 1992), [ANSI X3.92-1981(R1987)]
FIPS 48	Guidelines on Evaluation of Techniques for Automated Personal Identification, 1 April 1977
FIPS 49	Guideline on Computer Performance Management: An Introduction, 1 May 1977

12 Updated September 1993.

FIPS 53	Transmittal form for Describing Computer Magnetic Tape File Properties, 1 April 1978
FIPS 55 DC-4	Guideline: Codes for Named Populated Places, Primary Country Divisions, and Other Locational Entities of the United States and Outlying Areas, 16 January 1987, [ANSI X3.47-1988]
FIPS 55-2	Guideline: Codes for Named Populated Places, Primary Country Divisions, and Other Locational Entities of the United States, 3 February 1987, [ANSI X3.47-1988]
FIPS 56	Guideline for Managing Multivendor Plug-Compatible ADP systems, 15 December 1978
FIPS 57	Guidelines for the Measurement of Interactive Computer Service Response Time and Turnaround Time, 1 August 1978
FIPS 58-1	Representations of Local Time of the Day for Information Interchange, 27 January 1988, [ANSI X3.43-1986]
FIPS 59	Representations of Universal Time, Local Time Differentials, and United States Time Zone References for Information Interchange, 1 February 1979, [ANSI X3.51-1975]
FIPS 66	Standard Industrial Classification (SIC) Codes, 15 August 1979
FIPS 64	Guidelines for Documentation of Computer Programs and Automated Data Systems for the Initiation Phase, 1 August 1979
FIPS 65	Guideline for Automatic Data Processing Risk Analysis, 1 August 1979
FIPS 68-2	Basic, 28 August 1987, [ANSI X3.113-1987]
FIPS 69-1	FORTRAN, 24 December 1985, [ANSI X3.9-1978(R1990]
FIPS 70-1	Representation of Geographic Point Locations for Information Interchange, 14 November 1986, [ANSI X3.61-1986]
FIPS 71	Advanced Data Communication Control Procedures (ADCCP), 14 May 1980
FIPS 72	Guidelines for the Measurement of Remote Batch Computer Service, 1 May 1980
FIPS 73	Guidelines for Security of Computer Applications, 30 June 1980
FIPS 74	Guidelines for Implementing and Using the NBS Data Encryption Standard, 1 April 1981
FIPS 75	Guideline on Constructing Benchmarks for ADP System Acquisitions, 18 September 1980
FIPS 76	Guideline for Planning and Using a Data Dictionary System, 20 August 1980
FIPS 77	Guideline for Planning and Management of Database Applications, 1 September 1980
FIPS 78	Guideline for Implementing Advanced Data Communication Control Procedures (ADCCP), 26 September 1980
FIPS 79	Magnetic Tape Labels and File Structure for Information Interchange, 17 October 1980, [ANSI X3.27-1978]
FIPS 81	DES Mode of Operation, 2 December 1980
FIPS 83	Guideline on User Authentication Techniques for Computer Network Access Control, September 1980
FIPS 87	Guidelines for ADP Contingency Planning, 27 March 1989
FIPS 88	Guideline on Integrity Assurance and Control in Database Administration, 14 August 1980
FIPS 92	Guideline for Standard Occupational Classification (SOC) Codes, 24 February 1983
FIPS 95	Codes for the Identification of Federal and Federally-Assisted Organizations, 23 December 1982
FIPS 96	Guideline for Developing and Implementing a Charging System for Data Processing Services, 6 December 1982
FIPS 99	Guideline: A Framework for the Evaluation and Comparison of Software Development Tools, 31 March 1983
FIPS 100-1	Interfaces Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Operation with Packet-Switched Data Networks (PSDN), or Between Two DTEs, by Dedicated Circuit, NIST, US Department of Commerce, 20 March 1991 [ANSI X3.100-1989, ITU-TS X.25-1988, ISO 7776-1986, and ISO 8208-1987]
FIPS 101	Guideline for Lifecycle Validation, Verification, and Testing of Computer Software, 6 June 1983
FIPS 102	Guideline for Computer Security Certification and Accreditation, 27 September 1983
FIPS 103	Codes for the Identification of Hydrologic Units in the United States and the Caribbean Outlying Areas, 15 November 1983, [ANSI X3.145-1986]
FIPS 104-1	ANS Codes for the Representation of Names of Countries, Dependencies, and Areas of Special Sovereignty for Information Interchange, 1`2 May 1986, [ANSI Z39.27-1984]
FIPS 105	Guideline for Software Documentation Management, 6 June 1984
FIPS 106	Guideline on Software Maintenance, 15 June 1984
FIPS 107	Local Area Networks: Baseband Carrier Sense Multiple Access with Collision Detection Access Method and Physical Layer Specifications and Link Layer Protocol, NIST, US Department of Commerce, 31 October 1984
FIPS 109	Pascal, 16 January 1985
FIPS 110	Guideline for Choosing a Data Management Approach, 11 December 1984
FIPS 112	Password Usage, 30 May 1985
FIPS 113	Computer Data Authentication, 30 May 1985
FIPS 118	Flexible Disk Cartridge Labelling and File Structure for Information Interchange, 30 September 1985 [ISO 7665]
FIPS 119	Ada, 8 November 1985, [ANSI/MIL-STD 1815A-1983]

FIPS 120-1	Graphical Kernel System, 8 January 1991
FIPS 121	Videotext/Teletext Presentation Level Protocol Syntax (PLPS), (ANSI X3.110)
FIPS 122	Conformance Tests for FIPS PUB 100 Version of ITU-TS 1980 Recommendation X.25 Interface Between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Operation with Packet-Switched Data Communications Networks, 28 May 1986
FIPS 123	Specification for a Data Descriptive File for Information Interchange (DDF), 19 September 1986, [ANSI/ISO 8211-1985]
FIPS 124	Guideline on Functional Specifications for Database Management Systems, 30 September 1986
FIPS 125	MUMPS, 4 November 1986
FIPS 126	Database Language NDL, 10 March 1987
FIPS 127-2	Database Language SQL, 02 February 1992, [ANSI X3.135-1986]
FIPS 128	Computer Graphics Metafile (CGM), 16 March 1987, [ANSI X3.122-1986]
FIPS 132	Guideline for Software Verification and Validation Plans, 19 November 1987
FIPS 133	Coding and Modulation Requirements for 2400 Bit/Second Modems, 2 June 1986
FIPS 134-1	Coding and Modulation Requirements for 4800 Bit/Second Modems, 4 November 1988
FIPS 135	Coding and Modulation Requirements for Duplex 9600 Bit/Second Modems, March 1981
FIPS 136	Coding and Modulation Requirements for Duplex 600 and 1200 Bit/Second Modems, 16 June 1980
FIPS 137	Analog to Digital Conversion of Voice by 2,400 Bit/Second Linear Predictive Coding, 28 November 1984
FIPS 138	Electrical Characteristics of Balanced Voltage Digital Interface Circuits, 24 December 1975
FIPS 139	Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications, 3 August 1983
FIPS 140	General Security Requirements for Equipment Using the Data Encryption Standard, 14 April 1982
FIPS 141	Interoperability and Security Requirements for Use of the Data Encryption Standard with ITU-TS Group 3 Facsimile Equipment, 4 April 1985
FIPS 142	Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits, 31 January 1980
FIPS 143	General Purpose 37-Position and 9-Position Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment, 10 June 1985 (Reaffirmed 1-112-89)
FIPS 144	Data Communications Systems and Services User-Oriented Performance Parameters, 28 May 1985, [ANSI X3.102-1983 (R1990)]
FIPS 146-1	Government Open Systems Interconnection Profile (GOSIP), FIPS 146-1, Version 2.0, U.S. National Institute of Standards and Technology, 3 April 1991 (the 1994 version of GOSIP will point to the IGOSS specification; publication is being delayed to consider recommendations on the inclusion of TCP/IP and associative coexistence and convergence issues)
FIPS 147	Group 3 Facsimile Apparatus for Document Transmission, 19 August 1981
FIPS 148	Procedures for Document Facsimile Transmission, 14 April 1982
FIPS 149	General Aspects of Group 4 Facsimile Apparatus, 4 November 1988
FIPS 150	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus, 4 November 1988
FIPS 151-1	POSIX, 28 March 1990 [IEEE 1003.1-1988]
FIPS 152	Information Processing - Text and Office Systems - Standard Generalized Markup Language (SGML), 26 September 1988 [ISO 8879-1986]
FIPS 153	PHIGS, 14 October 1988, [ANSI/ISO 9592.1,2,3-1989 and ANSI/ISO 9693.1&3-1990]
FIPS 154	High Speed 25-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, 4 November 1988
FIPS 155	Data Communication Systems and Services User-Oriented Performance Measurement Methods, 4 November 1988, [ANSI X3141-1987]
FIPS 156	Information Resource Directory System (IRDS), 05 April 1989 [ANSI X3.138-1988]
FIPS 158	The User Interface Component of the Applications Portability Profile, 29 May 1990
FIPS 159	Detail Specification for 62.5-um Code Diameter/125-um Cladding Diameter Class IA Multimode, Graded-Index Optical Waveguide Fibers, 27 December 1990
FIPS 160	Information Systems - Languages - Programming Language C, 13 March 1991 (ISO 9899: 1990; ANSI X3.159-1989)
FIPS 161	Electronic Data Interchange (EDI), 29 March 1991
FIPS 171	Key Management Using ANSI X9.17, 27 April 1992
FIPS 172	VHSIC Hardware Description Language (VHDL), ANSI/IEEE 1076-1987, 29 June 1992
FIPS 173	Spatial Data Transfer Specification (SDTS), 15 February 1992 [DIS 10180]
FIPS 177	Initial Graphics Exchange Specification (IGES), ASME/ANSI Y14.26M-1989, 30 November 1992
FIPS 178	Video Teleconferencing Services at 56 to 1,920 kbit/s, ITU-TS Series H Recommendations H.221; 230; 242; 261; 320-1990, 30 November 1992
FIPS 179	Government Network Management Profile (GNMP), 14 December 1992
FIPS IDEF1X	Specifications for Integration Definition for Information Modeling (IDEF1X), 9 September 1992, Draft
FIPS ISDN	Integrated Services Digital Network [ITU-TS Series I], planned FIPS

FIPS TFA	Transparent File Access (TFA) [IEEE P1003.8], planned FIPS
IGOSS	The Industry/Government Open Systems Specification (IGOSS), Draft, IGOSS Panel, January 1994 (expected to be published as Version 1 in 1994; IGOSS is a joint effort by the US Government, the Canadian Government, MAP Users Group, TOP Users Group, and the Electric Power Research Institute)
Stable Agreements	Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 2, Edition 1, NIST Special Publication 500-16, National Institute of Standards and Technology, December 1988 (basis for U.S. GOSIP 1.0)
Stable Agreements	Stable Implementation Agreements for Open Systems Interconnection Protocols, Version 3, Edition 1, NIST Special Publication 500-177, National Institute of Standards and Technology, March 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop; basis for U.S. GOSIP 2.0)
Working Agreements	Working Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements, Volume 2, Number 2, NISTIR 90-4247, National Institute of Standards and Technology, February 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop)
Yellow Book	Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (Yellow Book), CSC-STD-003-85, DoD Computer Security Center, June 1985
Yellow Book Rationale	Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-85, DoD Computer Security Center, June 1985
Orange Book	Department of Defense Trusted Computer System Evaluation Criteria (Orange Book), DoD 5200.28-STD, DoD Computer Security Center, December 1985
Red Book	Trusted Network Interpretation (Red Book), NCSG-TG-005, Version 1, National Computer Security Center, July 1987
SDN.301	Secure Data Network System (SDNS) Security Protocol 3 (SP3), Revision 1.5, SDNS Protocol and Signalling Working Group, 15 May 1989, National Security Agency, UNCLASSIFIED
SDN.401	Secure Data Network System (SDNS) Security Protocol 4 (SP4), Revision 1.3, SDNS Protocol and Signalling Working Group, 2 May 1989, National Security Agency, UNCLASSIFIED
SDN.601	Secure Data Network System (SDNS) Key Management Profile, Communication Protocol Requirements for Support of the SDNS Key Management Protocol, Revision 1.5, SDNS Protocol and Signalling Working Group, 11 August 1989, National Security Agency, UNCLASSIFIED
SDN.701	Secure Data Network System (SDNS) Message Security Protocol (MSP), Revision 1.5, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN.702	Secure Data Network System (SDNS) Directory Specifications for Utilization with the SDNS Message Security Protocol (MSP), Revision 1.4, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN.801	Secure Data Network System (SDNS) Access Control Concept Document, Revision 1.3, SDNS Protocol and Signalling Working Group, 26 July 1989, National Security Agency, UNCLASSIFIED
SDN.802	Secure Data Network System (SDNS) Access Control Specification, Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency, UNCLASSIFIED
SDN.802/1	Secure Data Network System (SDNS) Access Control Specification, Addendum 1, Access Control Information Specification (ACIS), Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency, UNCLASSIFIED
SDN 902	Secure Data Network System (SDNS) Key Management Protocol, Definition of Services Provided by the Key Management Application Service Element (KMASE), Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN 903	Secure Data Network System (SDNS) Key Management Protocol, Specification of the Protocol for Services Provided by the Key Management Application Service Element (KMASE), Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency, UNCLASSIFIED
SDN 906	Secure Data Network System (SDNS) Key Management Protocol, SDNS Traffic Key Attribute Negotiation, Revision 1.3b, SDNS Protocol and Signalling Working Group, 18 September 1989, National Security Agency, UNCLASSIFIED

(This page intentionally left blank)

APPENDIX I

STANDARDS FOR PROFILES IDENTIFIED IN THE NOSIP STRATEGY

STANDARDS FOR PROFILES IDENTIFIED IN THE NOSIP STRATEGY

1. INTRODUCTION

The *NATO Open Systems Interconnection Profile (NOSIP) Strategy* [Ref. NATO 1993] has been developed by the Tri-Service Group on Communications and Electronics (TSGCE) and is expected to be promulgated in 1994 by the Conference of National Armaments Directors (CNAD). The NOSIP Strategy is an outgrowth of the *NTIS Transition Strategy* (Sixth Edition) [Ref. NATO 1991]. This appendix identifies the stacks of base standards specified in the *NOSIP Strategy* for example application, transport, and relay profiles. All are based on existing or emerging recommendations [e.g., International Standard Profiles (ISPs)] developed by international or regional standards bodies.

The notation used to identify and distinguish the functional profiles is that specified in ISO/IEC TR 10000. This taxonomy is described in Section 16.1.2.

2. APPLICATION PROFILES

2.1 Four file management functional profiles are shown in Figure I-1, all from ISP 10607:

(a) AFT11, Simple File Transfer

(b) AFT12, Positional File Transfer

(c) AFT22, Positional File Access

(d) AFT3, FTAM File Management

AFT11	
Application Layer	ISO 8571, ISO 8649, ISO 8650
Presentation Layer	ISO 8822, ISO 8823 ISO 8824, ISO 8825
Session Layer	ISO 8326, ISO 8327

(a) AFT11, Simple File Transfer

AFT12	
Application Layer	ISO 8571, ISO 8649, ISO 8650
Presentation Layer	ISO 8822, ISO 8823 ISO 8824, ISO 8825
Session Layer	ISO 8326, ISO 8327

(b) AFT12, Positional File Transfer

AFT22	
Application Layer	ISO 8571, ISO 8649, ISO 8650
Presentation Layer	ISO 8822, ISO 8823 ISO 8824, ISO 8825
Session Layer	ISO 8326, ISO 8327

(c) AFT22, Positional File Access

AFT3	
Application Layer	ISO 8571, ISO 8649, ISO 8650
Presentation Layer	ISO 8822, ISO 8823 ISO 8824, ISO 8825
Session Layer	ISO 8326, ISO 8327

(d) AFT3, FTAM File Management

Figure I-1. File Management Application Profiles

2.2 There are two Military Message Handling System (MMHS) application profiles identified in NOSIP Strategy, both derived from emerging STANAGs being developed by TSGCE Subgroup 9:

(a) AMH1x(M), MMHS Common Facilities, Table I-1

(b) AMH9x(M), MMHS Military Messaging, Table I-2 (the stacks are common to AMH1x(M).

Table I-1. AMH1x(M), MMHS Common Facilities

Layer	AMH11(M)	AMH12(M)	AMH13(M)
7	Draft STANAG 4404 ISO 9066-2 ISO 8650	Draft STANAG 4404 ISO 9072-2 ISO 9066-2 ISO 8650	Draft STANAG 4404 ISO 9066-2 ISO 8650
6	Draft STANAG 4266 (ISO 8823) Draft STANAG 4259 (ISO 8825) Draft STANAG 4258 (ISO 8824)	Draft STANAG 4266 (ISO 8823) Draft STANAG 4259 (ISO 8825) Draft STANAG 4258 (ISO 8824)	Draft STANAG 4266 (ISO 8823) Draft STANAG 4259 (ISO 8825) Draft STANAG 4258 (ISO 8824)
5	Draft STANAG 4265 (ISO 8237)	Draft STANAG 4265 (ISO 8237)	Draft STANAG 4265 (ISO 8237)

Table I-2. AMH9x(M), MMHS Military Messaging

Layer	AMH91(M)	AMH92(M)	AMH93(M)
7	Draft STANAG 4406 ISO 9066-2 ISO 8650	Draft STANAG 4406 ISO 9072-2 ISO 9066-2 ISO 8650	Draft STANAG 4406 ISO 9066-2 ISO 8650
6	Draft STANAG 4266 (ISO 8823) Draft STANAG 4259 (ISO 8825) Draft STANAG 4258 (ISO 8824)	Draft STANAG 4266 (ISO 8823) Draft STANAG 4259 (ISO 8825) Draft STANAG 4258 (ISO 8824)	Draft STANAG 4266 (ISO 8823) Draft STANAG 4259 (ISO 8825) Draft STANAG 4258 (ISO 8824)
5	Draft STANAG 4265 (ISO 8827)	Draft STANAG 4265 (ISO 8827)	Draft STANAG 4265 (ISO 8827)

2.3 Table I-3 identifies the stacks of standards for three system management profiles:

(a) AOM211, General Management Capability

(b) AOM221, General Event Report Control

(c) AOM231, General Log Control.

Table I-3. AMH9x(M), MMHS Military Messaging

Layer	AOM211	AOM221	AOM231
7	ISO 10164-1 ISO 10164-2 ISO 10164-3, 10164-4 ISO 10165-2 ISO 9595 ISO 9596-1 ISO 9072-1, 9072-2 ISO 8649, 8650 ISO 11183-1 ISO 11183-2	ISO 10164-1 ISO 10164-2 ISO 10164-5 ISO 10165-2 ISO 9595 ISO 9596-1 ISO 9072-1, 9072-2 ISO 8649, 8650 ISO 11183-1 ISO 11183-2	ISO 10164-1 ISO 10164-2 ISO 10164-6 ISO 10165-2 ISO 9595 ISO 9596-1 ISO 9072-1, 9072-2 ISO 8649, 8650 ISO 11183-1 ISO 11183-2
6	ISO 8822, 8823 ISO 8824, 8825 ISO 1183-1	ISO 8822, 8823 ISO 8824, 8825 ISO 1183-1	ISO 8822, 8823 ISO 8824, 8825 ISO 1183-1
5	ISO 8326, 8327 ISO 8326/AD2, 8327/AD2 ISP 11183-1	ISO 8326, 8327 ISO 8326/AD2, 8327/AD2 ISP 11183-1	ISO 8326, 8327 ISO 8326/AD2, 8327/AD2 ISP 11183-1

3. TRANSPORT PROFILES

Figure I-2 identifies 11 transport profiles. T-profiles use the connection-oriented transport service (COTS): TA involves the use of the connectionless network service (CLNS); TB, TC, and TD all involve the connection-oriented network service (CONS) and differ as to the required classes (TP0, TP2, TP4) of the COTS. [U-profiles (no examples given) use the connectionless mode transport service (CLTS)]. These transport profiles are:

(a) TA11x1, Permanent Access to a PSDN over a PSTN or a CSDN, Virtual Call (source: ISP 10608-5)

(b) TA51(M), COTS over CLNS in a LAN with CSMA/CD (military variant; sources: ISP 10608-2, STANAGs 4408-1, 4408-2, 4408-3)

(c) TA53, COTS over CLNS in Token Ring LAN with LLC1 (source ISP 10608-4)

(d) TA54(M), COTS over CLNS in FDDI LAN (military variant; sources ISP 10608-14, STANAGs 4408-1, 4408-2, 4408-3)

(e) TC11x1(M), COTS over CONS, Permanent Access to a PSDN via PSTN Leased Line [TC1111(M)] or Digital Data Circuit [TC1121(M)] (military variant; sources: STANAGs 4409-1, 4409-2, 4409-3)

(f) TC1231, ISDN B-Channel, Virtual Call, Switched Access to a PSDN (sources: ISP 10609-2, 10609-31)

(g) TC4111, ISDN B-Channel Semi-permanent Service, X.25 DTE to DTE (COTS and CONS) (sources: ISP 10609-2, 10609-32)

(h) TC4211, ISDN B-Channel Circuit-mode Service, X.25 DTE to DTE (COTS and CONS) (sources: ISP 10609-2, 10609-33)

(i) TC43111, ISDN D-Channel, Virtual Call, Packet-mode Service, Without X.931 (sources: ISP 10609-2, 10609-34) (see note below)

(j) TC43112, ISDN D-Channel, Virtual Call, Packet-mode Service, With X.931 (sources: ISP 10609-2, 10609-35)

(k) TC4331, ISDN B-Channel, Demand Access Virtual Call, Packet-mode Service (sources: ISP 10609-2, 10609-38).

The ISDN profile in Figure 1-2 (i) requires further study. The need for an ISDN-specific convergence-function sublayer, such as the one specified in ISO 9574 in profile TC 43111, requires further study because of the presence of a nailed-up virtual circuit.

TA11x1		
4	Transport Layer	ISO 8073 ISO 8073/AD2
3	Network Layer	ISO 8208 ISO 8473
2	Data Link Layer	ISO 7776
1	Physical Layer	CCITT X.21 CCITT X.21bis

Reference: ISP 10608-5.

(a) TA11x1, Permanent Access to a PSDN over a PSTN or a CSDN, Virtual Call

Figure I-2. Transport Functional Profiles

<table>
<tr><th colspan="3">TA51(M)</th></tr>
<tr><td>Transport Layer</td><td>STANAG 4264, Annex E
DIS 8073</td><td rowspan="3">TAnnnn (M) Group Profile: Part 1</td></tr>
<tr><td rowspan="3">Network Layer</td><td>STANAG 4263, Annex B
Trusted Communications Sublayer (TCS)</td></tr>
<tr><td>STANAG 4263, Annex E
ISO 8473 Subnetwork Independent Requirements</td></tr>
<tr><td>STANAG 4263, Annex E
ISO 8473 with ISO 8802
Subnetwork Dependent Convergence Function (SNDCF) and ISO 9542</td><td rowspan="2">TAnnnn (M) Profile: Part 2, TA5n (M)</td></tr>
<tr><td rowspan="2">Data Link Layer</td><td>STANAG 4262, Annex E
ISO 8802-2 (LLC)</td></tr>
<tr><td>STANAG 4262, Annex E
ISO 8802-3 (MAC)</td><td rowspan="2">TAnnnn (M) Profile: Part 3, TA51 (M)</td></tr>
<tr><td>Physical Layer</td><td>STANAG 4261
ISO 8802-3 (LPs, AUI, MAU)</td></tr>
</table>

References: ISP 10608-2; STANAGs 4408-1, 4408-2, 4408-3.

(b) TA51(M), COTS over CLNS in a LAN with CSMA/CD (Military Variant)

TA53		
4	Transport Layer	ISO 8073 ISO 8073/AD 2
3	Network Layer	ISO 8473 ISO 9542
2	Data Link Layer	ISO 8802-2 Type 1 ISO 8802-5 (MAC)
1	Physical Layer	ISO 8802-5 (PHY)

Reference: ISP 10608-4.

(c) TA53, COTS over CLNS in Token Ring LAN with LLC1

<table>
<tr><th colspan="4">TA54(M)</th></tr>
<tr><td>Transport Layer</td><td colspan="2">STANAG 4264, Annex E
DIS 8073</td><td rowspan="3">TAnnnn (M) Group Profile: Part 1</td></tr>
<tr><td rowspan="3">Network Layer</td><td colspan="2">STANAG 4263, Annex B
Trusted Communications Sublayer (TCS)</td></tr>
<tr><td colspan="2">STANAG 4263, Annex E
ISO 8473 Subnetwork Independent Requirements</td></tr>
<tr><td colspan="2">STANAG 4263, Annex E
ISO 8473 with ISO 8802
Subnetwork Dependent Convergence Function (SNDCF) and ISO 9542</td><td rowspan="2">TAnnnn (M) Profile: Part 2, TA5n (M)</td></tr>
<tr><td rowspan="2">Data Link Layer</td><td colspan="2">STANAG 4262, Annex E
ISO 8802-2 (LLC)</td></tr>
<tr><td>STANAG 4262, Annex E
ISO 8802-3 (MAC)</td><td rowspan="2">ANSI X3T9.5
FDDI SMT</td><td rowspan="2">TAnnnn (M) Profile: Part 4, TA54 (M)</td></tr>
<tr><td>Physical Layer</td><td>STANAG 4261
ISO 9314-1 (PHY)
STANAG 4261
ISO 9314-3 (PMD)</td></tr>
</table>

References: ISP 10608-14, STANAGs 4408-1, 4408-2, 4408-3.

(d) TA54(M), COTS over CLNS in FDDI LAN (Military Variant)

Figure I-2. Transport Functional Profiles (Cont'd)

<table>
<tr><th colspan="4">TC11x1(M)</th></tr>
<tr><td>Transport Layer</td><td>STANAG 4264, Annex E
ISO 8073</td><td rowspan="3">TCnnnn (M)
Group
Profile</td><td rowspan="6">TC1111(M) /
TC1121 (M)
Profile</td></tr>
<tr><td rowspan="3">Network Layer</td><td>STANAG 4263, Annex B; Trusted Communications Sublayer (TCS)</td></tr>
<tr><td>STANAG 4263, Annex C
ISO 8878
(Subnetwork-type independent requirements)</td></tr>
<tr><td>STANAG 4263, Annex C
ISO 8878, ISO 8208
(Subnetwork-type dependent requirements)</td><td rowspan="3">XX1111 (M) /
XX1121 (M)
Profile</td></tr>
<tr><td>Data Link Layer</td><td>STANAG 4262, Annex D
ISO 7776</td></tr>
<tr><td>Physical Layer</td><td>STANAG 4261
CCITT X.21, CCITT X.21bis</td></tr>
</table>

References: STANAGs 4409-1, 4409-2, 4409-3.

(e) TC11x1(M), COTS over CONS, Permanent Access to a PSDN via PSTN Leased Line [TC1111(M)] or Digital Data Circuit [TC1121(M)]

<table>
<tr><th colspan="5">TC1231</th></tr>
<tr><td>4</td><td colspan="2">Transport Layer</td><td colspan="2">ISO 8073 (Classes 0 and 2)</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">Network Layer</td><td>3c</td><td colspan="2">ISO 9574</td></tr>
<tr><td>3b</td><td rowspan="2">CCITT Q.931</td><td>ISO 8878</td></tr>
<tr><td>3a</td><td>ISO 8208 (X.25 PLP)</td></tr>
<tr><td>2</td><td colspan="2">Data Link Layer</td><td>CCITT Q.921 (LAP D)</td><td>ISO 7776 (LAP B)</td></tr>
<tr><td>1</td><td colspan="2">Physical Layer</td><td colspan="2">CCITT I.430 / I.431</td></tr>
<tr><td></td><td colspan="2"></td><td>D-Channel (control plane)</td><td>B-Channel (user plane)</td></tr>
</table>

References: ISP 10609-2, 10609-31.

(f) TC1231, ISDN B-Channel, Virtual Call, Switched Access to a PSDN

TC4111		
4	Transport Layer	ISO 8073 (Classes 0 and 2)
3	Network Layer	ISO 8208 ISO 8878
2	Data Link Layer	ISO 7776
1	Physical Layer	I.430 / I.431 B-Channel

References: ISPs 10609-2, 10609-32.

(g) TC4111, ISDN B-Channel Semi-permanent Service, X.25 DTE to DTE (COTS and CONS)

Figure I-2. Transport Functional Profiles (Cont'd)

TC4211				
4	Transport Layer		ISO 8073 (Classes 0 and 2)	
3	Network Layer	3c	ISO 9574 DAM 1	
		3b	CCITT Q.931	ISO 8878
		3a		ISO 8208 (X.25 PLP)
2	Data Link Layer		CCITT Q.921 (LAP D)	ISO 7776 (LAP B)
1	Physical Layer		CCITT I.430 / I.431	
			D-Channel (control plane)	B-Channel (user plane)

References: ISP 10609-2, 10609-33.

(h) TC4211, ISDN B-Channel, Circuit-mode Service, X.25 DTE to DTE (COTS and CONS)

TC43111			
4	Transport Layer		ISO 8073 (Classes 0 and 2)
3	Network Layer	3c	See text
		3b	ISO 8878
		3a	ISO 8208 (X.25 PLP)
2	Data Link Layer		CCITT Q.921 (LAP D)
1	Physical Layer		CCITT I.430 / I.431
			D-Channel (control plane) (user plane)

References: ISP 10609-2, 10609-34.

(i) TC43111, ISDN D-Channel, Virtual Call Packet-mode Service, Without X.931

TC43112				
4	Transport Layer		ISO 8073 (Class 0)	
3	Network Layer	3c	ISO 9574	
		3b	CCITT Q.931	ISO 8878
		3a		ISO 8208 (X.25 PLP)
2	Data Link Layer		CCITT Q.921 (LAP D)	
1	Physical Layer		CCITT I.430 / I.431	
			D-Channel (control plane)	(user plane)

References: ISP 10609-2, 10609-34.

(j) TC43111, ISDN D-Channel, Virtual Call Packet-mode Service, With X.931

TC4331				
4	Transport Layer		ISO 8073 (Classes 0 and 2)	
3	Network Layer	3c	ISO 9574	ISO 8878
		3b	CCITT Q.931	ISO 8208 (X.25 PLP)
		3c		ISO 7776 (LAP B)
2	Data Link Layer		CCITT Q.921 (LAP D)	
1	Physical Layer		CCITT I.430 / I.431	
			D-Channel	B-Channel

References: ISP 10609-2, 10609-38.

(k) TC4331, ISDN B-Channel, Demand Access Virtual Call, Packet-mode Service

Figure I-2. Transport Functional Profiles (Cont'd)

4. RELAY PROFILES

Figure I-3 identifies two relay profiles. These are:

(a) RA51.11x1, Relaying the CLNS, CSMA/CD LAN to PSDN Virtual Call
(b) RA51.51, Relaying the CLNS, CSMA/CD LAN to CSMA/CD LAN
(c) RA51.11x1, Relaying the X.25 Packet Layer Protocol, CSMA/CD LAN to PSDN Virtual Call
(b) RD51.51, Relaying the MAC Service Using Transport Bridging, CSMA/CD LAN to CSMA/CD LAN.

RA51.11x1			
	ISO 8473, ISO 9542		
Network Layer			ISO 8208
Data Link Layer	ISO 8802-2 Type 1 ISO 8802-3 (MAC)		ISO 7776
Physical Layer	ISO 8802-3 (PHY)		CCITT X.21, X.21bis, V-Series

Reference: DISPs 10613-8, 10613-9.

(a) RA51.11x1, Relaying the CLNS, CSMA/CD LAN to PSDN Virtual Call

RA51.51			
Network Layer	ISO 8473		ISO 9542
Data Link Layer	ISO 8802-2 Type 1 ISO 8802-3 (MAC)		ISO 8802-2 Type 1 ISO 8802-3 (MAC)
Physical Layer	ISO 8802-3 (PHY)		ISO 8802-3 (PHY)

Reference: DISP 10613-5.

(b) RA51.51, Relaying the CLNS, CSMA/CD LAN to CSMA/CD LAN

RC51.11x1			
Network Layer	ISO 8208 ISO 8881	ISO TR 10029	ISO 8208
Data Link Layer	ISO 8802-2 type 2 ISO 8802-3 (MAC)		ISO 7776
Physical Layer	ISO 8802-3 (PHY)		CCITT X.21 X.21bis, V-series

Reference: ISPs 10613-5, 10613-6.

(c) RC51.11x1, Relaying the X.25 Packet Layer Protocol, CSMA/CD LAN to PSDN Virtual Call

Figure I-3. Relay Functional Profiles

RD51.51			
Data Link Layer (MAC Sublayer)	ISO 8802-3 (MAC)	ISO 10038	ISO 8802-3 (MAC)
Physical Layer	ISO 8802-3 (PHY)		ISO 8802-3 (PHY)

Reference: ISP 10612-4.

(d) RD51.51, Relaying the MAC Service Using Transport Bridging, CSMA/CD LAN to CSMA/CD LAN

Figure I-3. Relay Functional Profiles (Cont'd)

APPENDIX J

MILITARY ENHANCEMENTS FOUND IN OSI STANAGS

MILITARY ENHANCEMENTS FOUND IN OSI STANAGS

1. STATUS OF NATO OSI STANAGS

Table J-1 identifies the STANAGs being developed that will specify ISO standards and applicable military options and extensions, if any. Work has begun on all these STANAGs, but only the NATO Reference Model, STANAG 4250, has been ratified. Originally, TSGCE SG9 planned to issue a single STANAG for all services and a second STANAG for all protocols at each layer, giving a total of 14 STANAGs in addition to STANAG 4250, the NATO Reference Model. In October 1987, TSGCE SG9 agreed [Ref. UK 1988, Annex 1.2] to work at the Application Layer for single STANAGs for each Application Layer service, such as MMHS (STANAG 4406). Protocol specifications as well as service definitions would be addressed in that STANAG.

Little progress on the lower layer STANAGs has been made during the past two years. Most of the changes observed on the various drafts of these documents during this period have been editorial. In a few cases, some PICS proformas have been added. Since these documents, for the most part, adopt international standards without enhancements, it is not clear why these standards were not released for ratification in 1991. The need for the layer STANAGs is not clear, especially if their primary role is to provide cover sheets for international civil standards.

Table J-1. NATO OSI Standards

Relation to OSI	Service Definitions			Protocol Specifications		
	STANAG	Status	Doc. Date	STANAG	Status	Doc. Date
Reference Model	4250, 4250-1	Ratified	21 August 1990		N/A	
	4250-2	Staffing	December 1993		N/A	
	4250-3	Draft	21 March 1993		N/A	
	4250-4	Draft	26 April 1993		N/A	
	4250-5X	Cancelled	1992		N/A	
	4250-6X	Cancelled	1992		N/A	
	4250-5Y	Cancelled	October 1993		N/A	
Layer 1	4251	Staffing	30 April 1993	4261	Staffing	17 March 1993
Layer 2	4252	Staffing	26 March 1993	4262	Staffing	18 March 1993
Layer 3	4253	Draft	18 March 1993	4263	Draft	19 March 1993
Layer 4	4254	Staffing	19 March 1993	4264	Staffing	19 March 1993
Layer 5	4255	Ratified	22 January 1993	4265	Ratified	22 January 1993
Layer 6	4256	Ratified	22 January 1993	4266	Ratified	22 January 1993
	4258 (ASN.1)	Ratified	22 January 1993	4259 (ASN.1 BER)	Ratified	22 January 1993
Layer 7	4257	Staffing	November 1993	4267	Staffing	November 1993
Layer 7	4406 (MMHS)	Draft	November 1993		N/A	
Profile	4407 (Mgmt)	Draft	15 May 1993		N/A	
Profile	4408 (COTS/CLNS))	Draft	October 1993		N/A	
Profile	4409 (COTS/CLNS))	Draft	7 April 1993		N/A	
Profile	4410 (CLTS/CLNS))	Draft	7 April 1993		N/A	
Profile	4413 (CLTS/CLNS))	Draft	January 1993		N/A	

Note: Staffing means that a final draft has been submitted by Subgroup 9 to the NATO International Military Staff for translation and distribution to the nations for ratification.
Source: [Rannestad 1994].

2. PHYSICAL LAYER STANAGS

The two STANAGs (4251 and 4261) characterize all but three of the areas identified as "not envisioned to affect the Physical Layer." The areas in which enhancements are possible (network/systems management, security, robustness, and quality of service) are marked "military enhancements are for further study." STANAG 4261 notes that mechanical aspects require militarization but that specifications are for further study. STANAG 4261 provides NATO PICS proformas for ISO 2110, ISO 4903, and ISO 8802.3; details for ISO 8802.3 are left for further study. In addition, STANAG 4261 provides NATO PICS proformas for the following ITU-TS standards: V.5, V.6, V.710, V.11, V.28, and X.1 (Annex I states that a proforma for V.24 is provided but there is no proforma appendix for this standard).

3. DATA LINK LAYER STANAGS

STANAG 4252 will address, as does ISO 8886 upon which it is based, both CO and CL modes of service. Both draft (March 1993) STANAGs 4252 and 4262 identify deficiencies only in one area (management) for which no enhancements are identified; any enhancements would depend on ongoing work in ISO.

4. NETWORK LAYER STANAGS

STANAG 4253 (April 1993) is based on ISO 8348 *(Network Service Definition)*, including the three addenda, and thus provides for both connection-mode and connectionless data transmission. The Security Annex is classified; as provided in the NOSA document (see Section 8.1.3.2), it addresses services such as peer entity authentication, data origin authentication, access control, connection confidentiality, connectionless confidentiality, traffic flow confidentiality, connection integrity without recovery, and connectionless integrity. STANAG 4253 addresses the areas of deficiencies of the civil standards shown in Table J-2 for providing military feature enhancements.

Annex D to STANAG 4253 discusses the two types of addresses used in the Network Layer: (1) subnetwork address, which identifies a point of attachment to a subnetwork (e.g., an X.25 network) and (2) network address. The subnetwork address must be derivable from the network address, either directly using a field of the network address or indirectly using routing table or directory service. Annex D provides technical detail on network address syntax, structure of an network service access point address, NATO initial domain identifier format, and NATO address allocation scheme.

STANAG 4263 (April 1993) specifies provision of the OSI network service using the X.25 Packet Layer Protocol (PLP); application of X.75; and provision of connectionless service using ISO 8473. Use of X.25 PLP over an ISO 8802 LAN is not addressed.

The required military enhancements for providing CONS using the X.25 PLP (Annex C) are given in Table J-3. Appendix 1 to Annex C is the PICS proforma. Appendix 2 to Annex C provides a set of enhancements to X.25 for additional optional user facilities to meet military requirements for security, precedence, and preemption. They include (1) "default security level assignment (an optional user facility agreed for a period of time) to provide for the selection of default security level—the highest security level that may be associated with any virtual call at the DTE/DCE interface—from the list of security levels supported by the network provided"; (2) "security level selection and indication" that may be requested by a DTE for a given virtual call; (3) "default priority levels assignment"; and (4) "priority level selection and indication."

An enhancement for only one military feature (precedence and preemption) is specified in Annex D for interconnecting two packet-switched networks using CONS and the X.75 PLP. Procedures and formats for the enhancement are specified in Appendix 2 to Annex D. The enhancement includes introduction of two optional network utilities to augment the standard network utilities: security level selection and priority level selection.

Annex E to STANAG 4263 [*Connectionless Network Protocol (CLNP)*] defines an internet protocol (IP) providing the CLNS. The CLNP relies on the provision of an underlying CL-mode service by real subnetworks or data links. It is classified as a subnetwork-independent convergence protocol. The underlying CLNS may be obtained either directly from a CL-mode real subnetwork or indirectly through the operation of an appropriate subnetwork-dependent convergence function (SNDCF) or protocol (SNDCP) over a CL-mode real subnetwork. Annex E is based on ISO 8473 (Sections 3-9 and Annexes A-C) and provides extensions for the following three military features:

- <u>Security</u>. A security parameter can be provided in every CLNP protocol data unit (PDU) using the Security Option. This is described in Appendix 3 to Annex E.
- <u>Precedence and preemption</u>. Priority is realized through selection of a priority parameter in the options part of the PDU header. Use of the priority parameter is optional. When implemented for use within end systems and intermediate systems, the priority parameter may be used as a criterion for preempting memory and/or processing resources. This can be achieved by sorting queued traffic within end systems and intermediate systems during periods of anticipated or real congestion.

Preemption of resources can be achieved by discarding NPDUs. Encoding of the precedence and preemption parameter and the error conditions are specified in the STANAG.

- Multiendpoint connection. It is necessary to allocate and reserve address space for multicasting and broadcasting in IP; extensions to IP to implement and manage multicasting are still to be defined.[1] Concepts for multicast addresses are described in detail in the STANAG.

Table J-2. Areas of Deficiencies and Enhancements for STANAG 4253

(1)	Multihoming. In the interest of survivability, an end system, identified by a single "logical" network address, may need to be connected at several Subnetwork Points of Attachment (SNPAs) either with more than one link into the same subnetwork or with links into several subnetworks. Routing management functions will be needed in order to determine the SNPA to be used. Enhancements for routing management (if any), maintenance of connections, and data transfer processing are for further study. Annex D defines extensions for logical network addresses.
(2)	Mobile Hosts. This requirement is for end systems identified by a single logical address to be able to connect to different SNPAs, although only one connection may be in use at any one time. In this case it may not be possible to determine in advance which subnetwork links will be involved in establishing connections associated with a particular subscriber address. The Network Layer addressing is extended in this STANAG to support logical network addresses that may identify more than one NSAP. Enhancements for routing management (if any), maintenance of connections, and data transfer processing are for further study. Annex D defines extensions for logical network addresses.
(3)	Multiendpoint Connections. To economize on network bandwidth and increase speed of delivery, an application that involves sending the same data to a number of destinations will require a multi-addressing service (multipeer data transmission) within the Network Layer, which provides either selective addressing or broadcast facilities. The Network Layer addressing is extended in Annex D of this STANAG to support multicast addresses that may identify more than one NSAP. Enhancements for multipeer data transmission are for further study.
(4)	Internetworking. No deficiencies in the application of the civil internetworking standards to military requirements have been identified.
(5)	Management. Additional management facilities may be required to support the other military enhancements. Military enhancements of the ISO Network Layer management objects are for further study.
(6)	Security. The ability is required to signal the security label of each network connection and each connectionless service data unit. The security classification will remain constant throughout the life of a connection. Enhancements: the security label for a network connection or a connectionless service data unit may be signalled as a protection QOS parameter.
(7)	Robustness and Quality of Service. The ability to survive physical damage and denial of service attacks and to route around damaged or partitioned networks is required for military systems. Military enhancements to Network Layer management functions for robustness are for further study. No requirement for military enhancement for the Network Layer service for QOS has been identified.
(8)	Precedence and Preemption. No requirement for military enhancement has been identified beyond the priority QOS parameter defined in ISO 8348.
(9)	Real-Time Communications. Enhancements for real-time communications are for further study.

Source: *Draft STANAG 4253*, 19 April 1993, NATO UNCLASSIFIED.

Annex E on CLNP does not specify the use or non-use of multicasting or broadcasting, but the Annex allocates and reserves address space for these two capabilities. The discussion of multicast encoding addresses the following topics: multicast addresses for subnetworks, multicasting addressing for areas, multicasting addresses for domains, multicasting error conditions, and multicast subscription options (TBD).

Annex E also contains a draft PICS proforma (Appendix 1) and an informative discussion of CL network routing exchange protocols (Appendix 2). A four-page informative appendix (Appendix 3) discusses security options for CLNP—these options are based on logical extensions of appropriate fields (i.e., Basic Portion fields and Extended Portion fields) within the provisions of ISO 8473. A congestion notification function is also described in Annex E.

1 Draft STANAG 4263 identifies US DoD RFC 1054, *Host Extensions for IP (DoD) Multicasting*, as the source for descriptions of the required extensions to ISO IP. See Appendix H.

Table J-3. Military Enhancements Identified for Annex C of STANAG 4263

(1)	Security. The use of the network service Protection Quality of Service parameter to associate a security level with a network connection is for further study.
(2)	Precedence and preemption. Military systems using OSI protocols need to be able to signal priority of data transferred over a connection, the priority to gain a connection, and the priority to keep a connection. The priority thereby signalled may then be used to determine the precedence of data and to control the use of and allocation of network resources. Use of priority facility is optional in this STANAG, but may be enforced by specific profiles. Priority values are integers in the range 0 to 14, with 255 meaning "unspecified." Annex C specifies the procedures to be used when a subnetwork does and alternatively does not implement precedence and preemption facilities.
(3)	Multihoming. Multihoming may be achieved through the X.25 Hunt Group optional user facility, provided the SNPAs corresponding to the various "homes" can be defined as members of an X.25(1988) Hunt Group. The use of the Hunt Group facility for multihoming is transparent to the OSI network service user. Three types of Network Layer management facilities are specified in the STANAG to support the use of a Hunt Group: configuration, multihoming subscription options, and multihoming registration.

Source: *Draft STANAG 4263*, 19 April 1993, NATO UNCLASSIFIED.

5. TRANSPORT LAYER STANAGS

STANAG 4254 (March 1993) provides the transport service definition. The CO transport service (Annex C) is based on ISO 8072. The CL transport service (Annex D) is based on ISO 8072/AD1 (with the restriction that the note of paragraph 15.2.3 is not retained).

Annex E (informative) of STANAG 4254, *Real-Time Transport Service (RTTS)*, has been proposed to fulfill the real-time military features for NATO military systems. Specifically, RTTS is designed to offer more functionality to such services as connection service and data transfer service and to provide additional services such as synchronization and management. RTTS provides services for broadcasting, selective broadcasting, and concentration. Appendix 1 of Annex E, *Definition of the Real-Time Transport Service (RTTS) Provided by the Transfer Layer*, uses concepts, terminology, and structure similar to ISO 8072 for transport Classes 0, 1, and 2. RTTS appears to impact more than a single layer (Layer 4) and does not appear to fully conform to the Basic Reference Model ISO 7498.

Deficiencies and required enhancements in seven areas are noted in STANAG 4254 for both CO-mode and CL-mode transport services as shown in Table J-4 (internetworking is not applicable).

Table J-4. Deficiencies and Enhancements Identified for STANAG 4254

(1)	Multihomed and mobile host systems. The transport service is not impacted by these requirements. No enhancements are required.
(2)	Multiendpoint connections. The transport service does not provide any service or function related to multiaddressing. To specify the addresses of participants in a multipeer connectionless transmission, the Group Address can be resolved into a number of ordinary addresses or the address parameters in the service definition can be redefined to permit the use of a list of addresses rather than just one.
(3)	Network/system management functions. System management services and definitions of managed objects are in progress in ISO and seem suitable for the NATO environment. Some specific military objects and functions are to be defined.
(4)	Security. Security is addressed in a classified annex.
(5)	Robustness and Quality of Service (QOS). No enhancements are required. QOS parameters are provided for data transfer service enabling the user to control and check the QOS. This parameter is negotiated during the connection establishment phase.
(6)	Precedence and preemption. No enhancements required. A QOS parameter is provided to express the priority of a transport connection.
(7)	Real-time and tactical communications. In real-time communications [there is a] requirement to have short transit delay. There is also a requirement for such services as sampling process data transmission, periodic data transmission, and synchronization service, which are not provided by the ISO transport service. The requirement of a short transit delay implies no segmentation of data; the length of the TSDU must be limited for that type of communication. For real-time communications, the definition of services is for further study (it could be based on the Real-Time Transport Service in Annex E). For tactical communications, ISO transport services are suitable.

Source: *Draft STANAG 4254*, 19 March 1993, NATO UNCLASSIFIED.

STANAG 4264 (March 1993) provides the transport protocol specification. The connection-oriented transport protocol (Annex C) is based on ISO 8073. The deficiencies and enhancements to seven of the military features (internetworking does not apply) are given in Table J-5.

Table J-5. Deficiencies and Enhancements Identified for Annex C of STANAG 4264

(1)	Multihomed and mobile host systems. The protocol shall have the recovery mechanism of Classes 1, 3, or 4 in the case where the Network Service Provider releases the network connection each time the host system changes SNPA and the QOS requirement specifies low probability of unexpected connection release. If the Classes 0 or 2 are used, the recovery of the connection shall be provided either in the Network Layer or in the Application Layer. If a host system has more than one NSAP or needs the capability to maintain communication with hosts associated with multiple NSAPs, then it shall support Classes 1, 3, or 4 with the multihoming enhancements specified in Appendix 2 to Annex C. These enhancements allow a transport connection to be associated with multiple NSAP pairs and shall be used to meet the transport connection resilience requested by the transport service user.
(2)	Multiendpoint connections. Savings in time and bandwidth can only be achieved if mechanisms are introduced into layers that inherently possess the ability to support communications to multiple destinations simultaneously (Layers 2 and 3). At present, only individual addresses can be used by the CO transport protocol and group addresses or lists of addresses are not supported by this protocol, even in the case where such address schemes are offered by the Network Service.
(3)	Network/system management. Specific military managed objects for the Transport Layer will be specified when they are identified. They will be specified as extensions/modifications to the civilian managed objects.
(4)	Security. Security deficiencies and enhancements are specified in a classified annex.
(5)	Robustness and Quality of Service (QOS). Transport Layer specifications of the mechanisms needed to respect the QOS requirements are for further study.
(6)	Precedence and preemption. Annex C describes mechanisms for encoding a priority parameter, maintaining QOS, providing transport connection preemption, and defining additional reason values.
(7)	Real-time and tactical communications. The real-time transport protocol, used over a CONS, is to be defined. The real-time transport protocol, used over a CLNS will be defined in Annex F (informative); details are to be defined.

Source: *Draft STANAG 4264*, October 1991, NATO UNCLASSIFIED.

Annex D specifies the connectionless transport protocol, based on ISO 8602. Enhancements are the same as in Annex C (Table J-5 above) with the following two exceptions:

- Multihomed and Mobile Host Systems. Since no data acknowledgment is provided by the service, the protocol is not affected when a remote host system changes its SNPA and is not reachable temporarily.
- Precedence and Preemption. Transport Layer specifications of the mechanisms involved for the management of the priority are for further study.

Annex E specifies the connection-mode transport protocol over CONS, based on ISO 8073 and ISO 8073/AD2 (*Class Four Operation Over Connectionless Network Service*) using TP4. Enhancements are the same as in Annex C (Table J-5) with the following exception:

- Multihomed and Mobile Host Systems. In the case of hosts with multiple SNPAs and a single NSAP, the protocol specified in ISO 8073 and 8073/AD1 is adequate, provided there are automated network/system management mechanisms that manage SNPA changes and reconfigure the network service provider's routing function. Hosts that have multiple NSAPs or need to communicate with hosts having multiple NSAPs shall support the ISO 8073 and 8073/AD1 protocol, including the ability to associate a transport connection with more than one NSAP pair, as is explicitly stated in Appendix 2 to Annex C. The availability of additional NSAP pairs shall be used to meet the transport connection resilience requested by the transport service user.

Annex F of STANAG 4264, *Real-Time Transfer Protocol Over Connectionless Network Service*, is still to be defined. It is intended to be used with military real-time LANs, such as those specified by STANAG 3838 (based on MIL-STD-1553-B that is used as a data bus in aircraft systems). The RTTS protocol has been discussed as a new work item in SC6 but has not yet been registered in ISO. It is available under the French reference GAM-T-103-B.

6. SESSION LAYER STANAGS

The two Session Layer STANAGs (4255 and 4265) have been developed by WG2 with the US serving as editor. Both these STANAGs were ratified without military features.

STANAG 4255 is based on ISO 8326, *Basic Connection-Oriented Session Service Definition;* STANAG 4265 is based on ISO 8327, *Basic Connection-Oriented Session Protocol Specification.* Each has an annex reserved for connectionless session services. The only military deficiency areas identified in these draft STANAGs are for security and multiendpoint connection:

- Security. A mechanism for providing graceful closure may be required by NATO in the long term. At present, this requirement is insufficiently refined to allow a service realization. Therefore, no enhancement of ISO security measures can be provided at this time.
- Multiendpoint connection. ISO is currently considering multipeer data transmission requirements for the Session Layer. This activity will be monitored by the developer of this STANAG, and this paragraph will be updated as developments warrant. An enhancement requirement is contingent upon ongoing developments within ISO.

7. PRESENTATION LAYER STANAGS

The two Presentation Layer STANAGs (4256 and 4266), together with STANAGs for ASN.1 (STANAG 4258) and the Basic Encoding Rules (BER) for ASN.1 (STANAG 4259) have been ratified without military features.

STANAG 4256 is initially based on ISO 8822, *Connection-Oriented Presentation Service Definition*; STANAG 4266 is based on ISO 8823, *Connection-Oriented Presentation Protocol Specification.* Each has an annex reserved for connectionless session services. Potential deficiencies have been noted in three areas for these STANAGs:

- Security (Annex B). NOSA has placed additional security-related services in the Presentation Layer, but these are not yet defined in detail. Modifications are anticipated in the ISO standards following ISO 7498-2, which may meet the emerging military requirements. No security enhancement to the ISO Presentation Layer is currently available. However, as solutions are available this STANAG will be amended.
- Mobile hosts and multihomed systems. No deficiencies noted (subject to change dependent upon the ability of the lower layers to support this feature).
- Multiendpoint connection. Modifications will be needed to the Presentation Layer if multiendpoint connections are required in an implementation, but no specific requirements have yet been identified. Modifications will be made to the ISO standard once the multipeer data transmission work in ISO has been progressed.

No deficiencies were found in the ASN.1 (STANAG 4258) and ASN.1 BER (STANAG 4259) standards, and no enhancements were recommended. STANAG 4259 observed that additional sets of encoding rules for ASN.1 may be required for specific applications giving either compressed (minimum volume) or encrypted encodings. No specific requirements in this area were identified.

8. APPLICATION LAYER STANAGS

Two STANAGs (4257 and 4267) were originally planned to address application service elements, such as ROSE, RTSE, and ACSE. No drafts of these documents has yet been produced. Other STANAGs are being prepared separately for MMHS (4406), Systems Management (4407), etc.

APPENDIX K

DISTRIBUTION LIST

DISTRIBUTION LIST

	No. of Copies
Office of the Secretary of Defense	
Office of the Assistant Secretary of Defense (C3I) ATTN: Director, Theater & Tactical C3 The Pentagon, Room 3D174 Washington, DC 20301-3040	5
Office of the Assistant Secretary of Defense (C3I)—DASD C3 ATTN: Ms. Deborah Castleman The Pentagon, Room 3E194 Washington, DC 20301-3040	1
Office of the Assistant Secretary of Defense (C3I)—Dir. Telecommunications ATTN: Ms. Diane Fountaine The Pentagon, Room 3E187 Washington, DC 20301-3040	1
Office of the Assistant Secretary of Defense (C3I)—DASD Information Management ATTN: Ms. Cynthia Kendall The Pentagon, Room 3E240 Washington, DC 20301-3040	1
Office of the Assistant Secretary of Defense (C3I)—DASD Intelligence ATTN: Mr. Ernie Liska, Dir. Intelligence Requirements and Plans The Pentagon, Room 3C200 Washington, DC 20301-3040	1
Office of the Assistant Secretary of Defense (C3I)—Information Management ATTN: Mr. John Graves, Dep. Dir. C3I Crystal Gateway #2, Suite 910 1225 Jefferson Davis Highway Arlington, Virginia 22202	1
Office of the Assistant Secretary of Defense (C3I)—Information Management ATTN: IM/IT (Mr. Terry Hagle) Crystal Gateway #2, Suite 910 1225 Jefferson Davis Highway Arlington, Virginia 22202	1
Office of the Assistant Secretary of Defense (C3I)—Information Management ATTN: IM/IT (Mr. Bert Newlin) Crystal Gateway #2, Suite 910 1225 Jefferson Davis Highway Arlington, Virginia 22202	1

	No. of Copies
Office of the Assistant Secretary of Defense (C3I)—Information Management ATTN: IM/IT (Mr. Tom Bozek) Crystal Gateway #2, Suite 910 1225 Jefferson Davis Highway Arlington, Virginia 22202	1
ASD for Production Resources ATTN: DQSO (Mr. Robert Gagnon) Two Skyline Place, Room 1403 5203 Leesburg Pike Falls Church, VA 22041-3466	1
Assistant Secretary of Defense for Production and Logistics ATTN: DQSO (Mr. Tom Ballentine) 2 Skyline Place, Room 1403 5203 Leesburg Pike Falls Church, VA 22041-3466	1
Under Secretary of Defense for Acquisition Director, Tactical Systems ATTN: Mr. Frank Kendall The Pentagon, Room 3E1044 Washington, DC 20301	1
ASD/Test and Evaluation (DDR&E) ATTN: Mr. Rod Knecht The Pentagon, Room 3E1064 Washington, DC 20301-3000	1
Defense CALS Executive ATTN: Ms. Elaine Litman The Pentagon, Room 3D833 Washington, DC 20301-3040	1
Joint Chiefs of Staff and Commands	
Joint Staff ATTN: J61 (LTC A. H. Whitley) The Pentagon, Room 2D860 Washington, DC 20301-5000	1
Joint Staff ATTN: J6I (CAPT John Ward, Jr.) The Pentagon, Room 1E833 Washington, DC 20301-5000	1
Joint Staff Joint Tactical C4 Systems Division ATTN: J6J (COL Elwood Jones) The Pentagon, Room 1D826 (Guard Post 10) Washington, DC 20301-5000	1

Joint Staff 1
ATTN: J6T (COL Marlin Forbes)
The Pentagon, Room 1D826 (Guard Post 10)
Washington, DC 20318-6000

Joint Staff 1
ATTN: J6V (LTC Michael Napoliello)
The Pentagon, Room 1D826 (Guard Post 10)
Washington, DC 20318-6000

Joint Staff 1
ATTN: J7 (COL Maurice L. McFann)
Joint Simulation and Interoperability Division
The Pentagon, Room 2B877G
Washington, DC 20318-6000

Joint Staff 20
Military Communications-Electronics Board
(DP and ES Panels)
ATTN: CDR Steve Soules
The Pentagon, Room 1E833
Washington, DC 20301-5000

US Atlantic Command 1
ATTN: J61 (CAPT Richard Stewart)
1562 Mitscher Avenue, Suite 200
Norfolk, VA 23551-2488

US Central Command 1
ATTN: CC/J6/D (LTC Michael Lemons)
7115 South Boundary Boulevard
Tampa, FL 33621-5101

US European Command 1
ATTN: ECJ6-D (Ms. Diane Gorzoch)
Unit 30400, Box 1000
APO AE 09128

US Forces Command 1
ATTN: FCJ6-P (Mr. Sammy L. Owens)
Fort McPherson, GA 30330-6000

US Pacific Command 1
Information Management Office
ATTN: J61, Box Rte 28 (Mr. Donald DeRyke)
Camp H. M. Smith, HI 96861-5025

US Pacific Command 1
Systems Integration Division
ATTN: J61 (Mr. Morris Johnson, Jr.)
Camp H. M. Smith, HI 96861

US Pacific Command 1
ATTN: J64 (CAPT Jim Day)
Camp H. M. Smith, HI 96861

US Space Command 1
ATTN: J4L (Col George J. Sawaya)
250 South Peterson Boulevard, Suite 116
Peterson Air Force Base, CO 80914-3050

US Strategic Command 1
ATTN: J63 (Mr. Ed Gleisberg; Mr. James Muckey)
901 SAC Boulevard, Suite 207
Offutt Air Force Base, NE 68113-6600

US Strategic Command 1
ATTN: J6-2KBS (COL Ron Hall; Mr. Al Fransen)
901 SAC Boulevard, Suite 281
Offutt AIR FORCE BASE, NE 68113-6600

US Transportation Command 1
ATTN: TCJ6-SP (COL Anthony W. Bell, Jr.)
508 Scott Drive
Scott Air Force Base, IL 62225-5357

US Transportation Command 1
ATTN: J3/J4-LPI (Mr. Michael Gilchrist)
508 Scott Drive
Scott Air Force Base, IL 62225-5357

US Mission/NATO Headquarters 2
Communications Electronics Division
ATTN: Dr. Gopa D. Hingorani
APO New York, NY 09667

NACISA (USDCFO) 1
US Defense Communications Field Office
ATTN: Mr. Elbert J. Wells, Frank Powers
APO AE 09724

NACISA (NSA) 1
ATTN: Mr. Richard Parker
PSC 79, Box 003
APO AE 09724

Defense Agencies and NSA

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
ATTN: TA (CAPT Phillip Bower, Deputy Director)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
NATO C3 Liaison Office
ATTN: TICC (Mr. Tom Kuntz)
Skyline 3, Suite 1501
5201 Leesburg Pike
Falls Church, VA 22041

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TF (Mr. Bruce Brown)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TFA (Mr. John Deitz)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TFB (Mr. Doug Epley)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TFC (Mr. John Mitchell)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TFC (Dr. William Vogelzang)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TFCC (Mr. Bryan Purdy)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TFCD (Dr. Mike McGreer)
Virginia Square Plaza
3701 N. Fairfax Drive
Arlington, VA 22203

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Architecture
ATTN: TFDB (Mr. Ed Richards)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Engineering
ATTN: TEF (Mr. E. M. Hanz)
Parkridge III
10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Engineering
ATTN: TEFD (Mr. George Bradshaw)
Parkridge III
10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Engineering
ATTN: TEFE (Mr. Edward Cain)
Parkridge III
10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Engineering
ATTN: TEFE (Mr. Robert Cleary)
Parkridge III
10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Engineering
ATTN: TEFE (Mr. James Showalter)
Parkridge III
10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Engineering
ATTN: TEFEE (Mr. Sherrill Adkins)
Parkridge III
10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Engineering
ATTN: TEWSA (Ms. Mary Jane Haley)
45335 Vintage Park Plaza
Sterling, VA 20166-6701

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Information Management
ATTN: TX (Ms. B. Leong-Hong)
701 South Court House Road
Arlington, Virginia 22204-2199

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Integrated Mission Support
ATTN: TD (Mr. Bob Leary)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Integrated Mission Support
ATTN: TDA (Mr. Herb Goertzel)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Integrated Mission Support
ATTN: TDB (Mr. Richard Moriarty)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Integrated Mission Support
ATTN: TDB (LTC M. E. Friel)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Integrated Mission Support
ATTN: TD (LTC Rick Zapka)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Integration and Interoperability
ATTN: TI (Dr. Mestrovich, Director)
Skyline 3, Suite 1501
5201 Leesburg Pike
Falls Church, VA 22041

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Integration and Interoperability
ATTN: TIC (COL Kent Schneider)
Skyline 3, Suite 1501
5201 Leesburg Pike
Falls Church, VA 22041

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TB (Dr. Jeremy Kaplan, Director)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TB (Ms. Marilyn Kraus)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBA (Mr. Joe Pasquariello, Associate Dir)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
Center for Standards, Information Transfer
Directorate
ATTN: TBB (Mr. Louis Pilla, Deputy Director)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBB (Library Copy)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBA (LtCol Harry Barksdale)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBB (Mr. Thomas J. Brincka)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBC (Mr. Edward F. Kovanic)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBD (Mr. Richard McLane)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 17
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBD (Mr. Walt Lucchesi, for distribution to
DTMP S/A voting members and WG chairs)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 2
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBF (Mr. Salvatore Manno)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBF (Dr. Frank Curcio)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
ATTN: TBBF Mr. Vincent Chin)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization,
Center for Standards
Directorate for DoD Standards Assistance
ATTN: TBD (Mr. Ramaswami, Deputy Director)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization, Center for Standards
ATTN: TBDA (Mr. David Sweet)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 5
Joint Interoperability and Engineering Organization, Center for Standards
ATTN: TBDB (LCDR Doug Schroeder)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization, Center for Standards
Information Processing Standards Directorate
ATTN: TBE (CAPT Richard Petersen, Dep. Dir)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

JSARO 1
ATTN: Army/Navy/USMC/AF/NSA/DIA
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization, Center for Standards
ATTN: TB (Mr. Gary Koerner)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization, Center for Standards
ATTN: TBC (Mr. Norton Bragg)
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
ATTN: TDF (Mr. Jimmie Lee)
11440 Isaac Newton Square, Suite 210
Reston, VA 22090-5006

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
ATTN: Mr. Alan Peltzman
Parkridge III Building, 10701 Parkridge Boulevard
Reston, VA 22091-4398

Director, Defense Information Systems Agency 1
Joint Interoperability and Engineering Organization
ATTN: TBBC (Mr. Bill Scott)
Building 286 (Russell Hall)
Fort Monmouth, NJ 07703-5613

Director, Defense Information Systems Agency 1
Defense Information Systems Management Ctr
Operations, Customer Relations, and Service
ATTN: Mr. John Edell, Acting Deputy Director
701 S. Court House Road
Arlington, VA 22204-2199

Director, Defense Information Systems Agency 1
Defense Network Systems Organization (DNSO)
701 S. Court House Road
Arlington, VA 22204-2199

Director, Defense Information Services Org. 4
ATTN: DISO/UAP (Mr. John Keane)
1951 Kidwell Drive
Vienna, VA 22182-3930

Director, Joint Interoperability Test Center 1
Tactical Communications Division
ATTN: JITC/TCB (Mr. Leo Hansen)
Fort Huachuca, AZ 85613-7020

Director, Joint Interoperability Test Center 1
Tactical Communications Division
ATTN: JITC/TCDB (Mr. Dwaine Huewe)
Fort Huachuca, AZ 85613-7020

National Communications System 1
ATTN: Code NT (Dennis Bodson, Frank McClelland, Robert Fenichel)
701 South Court House Road
Arlington, VA 22204-2198

Director, Defense Mapping Agency 3
ATTN: TI, Mail Stop A-10 (Mr. Charles Roswell)
8613 Lee Highway
Fairfax, VA 22031-2137

NATO Integrated Communications Systems Management Agency 1
NACISA
ATTN: USDCFO
APO AE 09724

Director, National Security Agency 3
ATTN: V5 (Mr. Harold Staton, Gerald Bailey)
9800 Savage Road
Fort George Meade, MD 20755-6000

Director, National Security Agency 2
ATTN: V3 (Mr. Dick McAllister)
Airport Square 10
Fort George Meade, MD 20755-6000

Director, National Security Agency 3
ATTN: I9 (Mr. Dale Nunley)
Airport Square 20
Fort George Meade, MD 20755-6000

Director, National Security Agency 1
ATTN: I11 (Mr. S. J. Buchanan)
OPS 3
Fort George Meade, MD 20755-6000

Director, National Security Agency 2
ATTN: R23 (Mr. Doug Maughan)
Fort George Meade, MD 20755-6000

Director, National Security Agency 1
ATTN: R536 (Mr. Ray McFarland)
Fort George Meade, MD 20755-6000

Director, National Security Agency 1
ATTN: I91 (Ms. Tammy Mannarino)
9800 Savage Road
Fort George Meade, MD 20755-6000

Director, Defense Intelligence Agency 2
DIA Management Board
ATTN: S-02 (Maj Gilbert Armour)
Washington, DC 20340-5100

Director, Defense Intelligence Agency 2
INCA Project Office
ATTN: Mail Stop W940 (Mr. George Endicott)
Washington Building
7798 Old Springhouse Road
McLean, VA 22102

Director, Defense Logistics Agency 1
ATTN: DLA-ZIA
Cameron Station
5010 Duke Street
Alexandria, VA 22312-6101

Director, Defense Logistics Agency 1
ATTN: DLA-ZID/DRDO (Mr. George Pogharian)
6303 Little River Turnpike at Beauregard Street,
Suite 310
Alexandria, VA 22312-5040

Director, Defense Logistics Agency 1
Systems Automation Center
ATTN: DSAC-RSB (Mr. Clyde Grossarth)
P. O. Box 1605
Columbus, OH 43216-5002

Ballistic Missile Defense Organization (BMDO) 1
The Pentagon, Room 1E1037
Washington, DC 20301-7100

Institute for National Strategic Studies 1
ATTN: Dr. Stuart Johnson, Dir Strategic Concepts
Development Center; Dr. Martin Libicki
National Defense University, Room 209
Fort McNair
Washington, DC 20319

Information Resources Management College 1
Department of Information Technology
ATTN: Dr. J. Couture, Chair
National Defense University, Room 136
Fort McNair
Washington, DC 20319

Armed Forces Staff College 1
C3 Division (AFSC-C3D)
ATTN: LtCol M. L. Vanpelt, Chair
Norfolk, VA

Director, DISA 1
ATTN: XL (Mr. Robert Compton)
P. O. Box 1605
Columbus, OH 43216-5002

US Coast Guard 1
ATTN: Comdt G-TA
2100 Second Street, SW
Washington, DC 20593-0001

Information Handling Committee, ICS
Mr. George W. Rogers, Jr., Vice-Chairman 1
Washington, DC 20505

Department of the Army

HQDA ODISC4 15
Interoperability and Standards Office
ATTN: SAIS-ADO (LTC D.S. Woffinden)
The Pentagon, Room 1C638
Washington, DC 20310-0107

HQDA ODISC4 1
Interoperability and Standards Office
ATTN: SAIS-ADO (Mr. L. Tom Hendrick)
The Pentagon, Room 1C638
Washington, DC 20310-0107

HQDA DCS Operations and Plans 1
Director of Requirements
ATTN: DAMO-FDQ (Mr. John Pijnowski)
The Pentagon, Room 3C481
Washington, DC 20310-0107

Commander, US Army Signal Center 1
Directorate of Combat Development
ATTN: ATZH-CD (COL Forrester)
Fort Gordon, GA 30905-5090

Commander, US Army Signal Center 1
Battle Command Battle Laboratories
ATTN: ATZH-BL (COL Nicholson)
Fort Gordon, GA 30905-5090

CINCUSAREUR 1
ATTN: AEAIM-AR-AR
APO AE 09403

Commander, US Army Pacific Command 1
ATTN: APIM-PRA (Mr. Joe Ng)
Fort Shafter, HI 96858-5100

Commanding General, U.S. Army TRADOC 1
ATTN: ATCD-CB (Mr. Richard Hill)
Fort Monroe, VA 23651-5000

Commanding General, U.S. Army TRADOC 1
Director of Information Management (DOIM)
ATTN: ATIM-IAP (Mr. Riley Best)
Fort Monroe, VA 23651-5000

Commanding General, U.S. Army TRADOC 1
ATTN: ATCD-GC (Mr. Phil Casey)
Fort Monroe, VA 23651-5000

Commander, USAISEC 1
ATTN: ASQB-OTD (Mr. Mike Gentry, Technical
Director)
Fort Huachuca, AZ 85613-5300

Director, US Army Information Systems
Command (USAISC) 1
Software Development Center
ATTN: ASQB-SIS (Mr. Dick Fair)
Fort Huachuca, AZ 85613-5450

Commander, USAISEC 1
ATTN: ASQB-SIS (Mr. Jim Starkey)
Fort Huachuca, AZ 85613-5300

Director, USAISC-Pentagon 1
ATTN: ASQNS-TS-D (Mr. Thomas J. Kenavan)
The Pentagon, Room BE1018
Washington, DC 20310-3053

Commander, USAISMA 1
ATTN: Mr. Frank Dwulet
Fort Monmouth, NJ 07703

Commander, US Army Operational Test and Evaluation Command 1
ATTN: Dr. Henry Dubin, Technical Director
Park Office Center, Room 1420
4501 Ford Avenue
Alexandria, VA 22302-1458

Headquarters, Department of the Army 1
PEO-IEW
ATTN: Mr. Dae-Woo Lee
VHFS
Warrenton, VA 22186-5115

US Army, PEO STAMIS 1
ATTN: SFAE-PS-S (Mr. Michael Falat)
Fort Belvoir, VA 22060-5895

Commander, U.S. Army Combined Arms Center 1
ATTN: ATZL-CDC-A (Mr. Frank Torres)
Ft. Leavenworth, KS 66027-3500

Commander, U.S. Army Combined Arms Center 1
ATTN: TSM-ACCS (COL Tom Dials, Cpt H. Matthews)
Building 52 (Grant Hall), Room 128
Ft. Leavenworth, KS 66027-3500

Director, US Army RDEC 1
ATTN: AMSEL-RD (Mr. Robert Giordano)
Building 1210
Ft. Monmouth, NJ 07703-5000

Director, US Army RDEC 1
Software Engineering Division
ATTN: AMSEL-RD-SE-D (Mr. Dennis Turner)
Building 1210
Ft. Monmouth, NJ 07703-5207

Director, US Army RDEC 1
Software Engineering Division
Command and Control Information Systems
ATTN: AMSEL-RD-C2-D (Mr. Bruce Miller)
Building 1210
Ft. Monmouth, NJ 07703-5207

Commander, CECOM 1
PEO Communications
ATTN: Mr. Neil Atkinson, Deputy PEO
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 1
ATTN: SFAE-CC/PEO CCS (MGen Campbell)
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 1
PM CHS
ATTN: SFAE-CC-CHS (Mr. Stan Levine)
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 1
ATTN: SFAE-CC/DPEO CCS (Mr. Mike Albarelli)
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 2
PM FATDS, Technical Management Directorate
ATTN: SFAE-CC-FS-TMD (Henry Saphow, Mike Simpson)
Building 549
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 1
PM OPTADS
ATTN: SFAE-CC-OPTDS (Mr. Paul Ulrick)
Ft. Monmouth, NJ 07703-5000

Director, Joint Tactical Fusion Program 1
ATTN: PM ASAS (Mr. Vince Drobney)
1616 Anderson Road
McLean, VA 22102-1616

Commander, CECOM 1
Software Engineering Directorate
ATTN: AMSEL-RD-SE-AIN (Mr. Jack Zavin)
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 1
ATTN: Mr. J. Onufer
Ft. Monmouth, NJ 07703-5000

Commander, CECOM 1
C2 Systems Integration Directorate
ATTN: AMSEL-RD-C2-PM (Mr. Jack Plant)
Ft. Monmouth, NJ 07703-5000

Department of the Army AIRMICS 1
ATTN: Mr. Winfred Fong, Dan Hocking
115 O'Keefe Building
Georgia Institute of Technology
Atlanta, GA 30332-0800

Commander AMC RDEC 1
ATTN: SMCAR-FSC (Dr. T. H. Chin)
Building 352 North
Dover, NJ 07801-5001

Commander, Corps of Engineers 1
Directorate of Information Management
Infrastructure Support Division
ATTN: CEIM-SE (Mr. Webster Smith)
Pulaski Building, Room 5120C
20 Massachusetts Avenue, NW
Washington, DC 20314-1000

Department of the Navy

Chief of Naval Operations 1
Director, Space and Electronic Warfare
ATTN: N6 (Dr. J. R. Davis, Chief Scientist)
The Pentagon, Room 4C671
Washington, DC 20350

Chief of Naval Operations 1
Director, Space and Electronic Warfare
Information Transfer Division
ATTN: N61 (COL Edward R. Palmquist, Jr.)
The Pentagon, Room 5A586
Washington, DC 20350

Chief of Naval Operations 1
Director, Space and Electronic Warfare
Information System Requirements
ATTN: N62 (CAPT William C. Liebe)
The Pentagon, Room 5E569
Washington, DC 20350

Chief of Naval Operations 1
Director, Space and Electronic Warfare
NCTS-A Requirements
ATTN: N62J (CDR James R. Kirkpatrick)
The Pentagon, Room 5E523
Washington, DC 20350

Chief of Naval Operations 1
Director, Space and Electronic Warfare
Tactical C3I Systems Interoperability Coord.
ATTN: N62T (Mr. J. D. Ferrell)
The Pentagon, Room 5E523
Washington, DC 20350

Chief of Naval Operations 1
Director, Space and Electronic Warfare
Information Resource Management Division
ATTN: N65 (CAPT P. A. Callahan)
The Pentagon, Room 5A734
Washington, DC 20350

HQ Department of the Navy 1
Navy Information System Management Center
ATTN: ADM Hakman, Commander; Rebecca Wade
Crystal Gateway #2
1225 Jefferson Davis Highway, Suite 1500
Arlington, VA 22245

HQ Department of the Navy 1
Navy Information System Management Center
ATTN: Code 03 (Marshall Potter, John Hooder)
Crystal Gateway #2
1225 Jefferson Davis Highway, Suite 1500
Arlington, VA 22245

HQ Department of the Navy 1
Information Technology Acquisition Center
ATTN: Robert A. Green, Standards Division
Washington Navy Yard, Building 176
Washington, DC 20374-1662

Commander, Space and Naval Warfare Systems
Command (SPAWAR) 1
ATTN: PD60 (CAPT J. A. Gauss)
Crystal Park #5, Room 30
2451 Jefferson Davis Highway
Arlington, VA 22245-5200

Commander, Space and Naval Warfare Systems
Command (SPAWAR) 1
ATTN: PMW-161 (CAPT Bostian)
Crystal Park #5, Room 421
2451 Crystal Drive
Arlington, VA 22245-5200

Commander, Space and Naval Warfare Systems
Command (SPAWAR) 1
ATTN: 231/2B3 (CDR Michael C. Aaby)
Crystal Park #5, Room 701
2451 Crystal Drive
Arlington, VA 22245-5200

Commander, Space and Naval Warfare Systems
Command (SPAWAR) 1
ATTN: 322-15 (Mr. Robert D. Kolacki)
Crystal Park #5, Room 701
2451 Crystal Drive
Arlington, VA 22245-5200

Commander, Naval Research Laboratory 1
ATTN: Code 910 (Robert Parks)
4555 Overlook Avenue, SW, Room 2650
Washington, DC 20375

Commander, Navy Center for Tactical Systems
Interoperability (NTCSI) 1
ATTN: Code 5A (Mr. Pete Whitby)
200 Catalina Boulevard
San Diego, CA 92152-5082

Director, NCCOSC RDTE Division 1
ATTN: Div 411 (Donna Fisher)
49180 Transmitter Road, Room 2
San Diego, CA 92152-7341

Commander, NUSC 1
ATTN: Code 2222 (Richard Leary)
Building 1171-3
Newport, RI 02841

Office of Naval Intelligence 1
ATTN: ONI-734 (Ms. Joyce Wineland)
4600 Silver Hill Road
Washington, DC 20389-5000

Office of Naval Technology 1
ATTN: Code 221 (Sherman Gee)
Ballston Center Towers #1, Room 503
800 North Quincy Street
Arlington, VA 22217-5000

Deputy Chief of Staff for Programs and Resources 1
US Marine Corps
Code R
Navy Annex, Room 3020
Washington, DC 20380

Assistant Chief of Staff, C4I Department, US Marine
Corps 1
ATTN: Code C4I (Mr. Ron Elliott)
Federal Building 2 (Navy Annex), Room 3234
Washington, DC 20380-1775

Assistant Chief of Staff, C4I Department, US Marine Corps 1
C4I Architecture & Standards Branch
ATTN: Code CSA (LtCol J. D. Inghram, Head))
Federal Building 2 (Navy Annex), Room 3201
Washington, DC 20380-0001

Assistant Chief of Staff, C4I Department, US Marine Corps 1
C4I Systems Branch
ATTN: Code CSB (Col J. E. Vesely, Head)
Federal Building 2 (Navy Annex), Room 3312
Washington, DC 20380-0001

Commander, Marine Corps Systems Command 2
ATTN: Director C4I (Col S. J. D'Lugos, Mr. Dan Walsh)
2033 Barnett Avenue
Marine Corps Base
Quantico, VA 22134-5010

Commander, Marine Corps Systems Command 2
Director C4I, C4I Interoperability and Integration
ATTN: C4I2&I
2033 Barnett Avenue, Suite 315
Marine Corps Base
Quantico, VA 22134-5010

Commanding General, Marine Corps Combat Development Command 1
ATTN: Requirements Division (Maj Imhof)
Marine Corps Base
Quantico, VA 22134

Director, MCOTEA 1
ATTN: ACTB (Maj Michael Mascarenas)
3035 Barnett Avenue
Marine Corps Base
Quantico, VA 22134-5014

Director, Marine Corps Computers and Telecommunications Activity (MCCTA) 1
ATTN: CTAS
Marine Corps Base
Quantico, VA 22134-5080

Director, Marine Corps Computers and Telecommunications Activity (MCCTA) 1
ATTN: Technical Director (Mr. Antonich)
Marine Corps Base
Quantico, VA 22134-5080

Commander, Marine Corps Tactical Systems Support Activity (MCTSSA) 1
ATTN: Col Chadwick, Commander; Mr. Jim Steenwerth
Camp Pendleton, CA 92055-5080

Department of the Air Force

HQ USAF, DCS C4 1
ATTN: AF/SCTA (MAJ Mike Pait)
The Pentagon, Room 5B513
Washington, DC 20330-1250

HQ USAF, DCS C4 1
ATTN: AF/SCTA (Mr. Fred Virtue)
The Pentagon, Room 5B513
Washington, DC 20330-5190

HQ USAF, DCS C4 1
Directorate of Mission Systems
ATTN: AF/SCM (Col Joseph M. Narsavage)
The Pentagon, Room 5B525
Washington, DC 20330

HQ USAF, DCS C4 1
Directorate of Plans and Policy, Policy Division
ATTN: AF/SCXX (LtCol Larry Cannon)
The Pentagon, Room 5B315
Washington, DC 20330-5190

HQ USAF, DCS Plans and Operations 1
Directorate of Forces, Combat Integration Div.
ATTN: AF/XOFI (Col. R. Stammler)
The Pentagon, Room 4C174
Washington, DC 20330

HQ USAF 1
Directorate of Operational Requirements
ATTN: AF/XOR (Col M. Ward, Deputy Director)
The Pentagon, Room 4E1021
Washington, DC 20330-5190

HQ USAF, Air Force Intelligence Agency 1
ATTN: AFISA/IND (Maj Mark Harris)
520 Bolling Air Force Base
Washington, DC 20332

HQ USAF 1
ATTN: SC/XPT (Ms. Elizabeth Crouse)
Gunter Air Force Base, AL 62225-6001

HQ USAF Electronic Systems Command 1
ATTN: ESC/AVB
9 Eglin Street
Hanscom Air Force Base, MA 01731-2110

HQ USAF Air Combat Command 1
ATTN: ACC/DRI-SD (Maj Thomas Spivey)
204 Dodd Boulevard, Suite 226
Langley Air Force Base, VA 23665-2777

HQ USAF Air Combat Command 1
ATTN: ACC/DRC
204 Dodd Boulevard, Suite 202
Langley Air Force Base, VA 23665-2777

HQ USAF Air Combat Command 1
ATTN: ACC/SCT
180 Benedict Avenue, Suite 209
Langley Air Force Base, VA 23665-1993

HQ USAF Space Command 1
ATTN: SYE (Capt Cosgrove)
Peterson Air Force Base, CO 80194-5001

HQ USAF Space Command 1
North American Air Defense Command
ATTN: IM
150 Bandenberg Street, Suite 1105
Peterson Air Force Base, CO 80194-4080

HQ USAF AFC4A 1
Computer Standards Office
ATTN: TNA (Mr. Rex McKinnon, Chief)
Scott Air Force Base, IL 62225-5421

HQ USAF AFC4A 1
Computer Standards Office
ATTN: TNABI (Ms. Sandra Swearingen)
607 Pierce Street, Room 303
Scott Air Force Base, IL 62225-5421

HQ USAF AFC4A 1
Computer Standards Office
ATTN: TNABP (Mr. Larry Messina)
607 Pierce Street, Room 300
Scott Air Force Base, IL 62225-5421

HQ USAF AFC4A 1
ATTN: XPPA (CMSgt B. T. Washington)
203 West Losey Street, Room 1020
Scott Air Force Base, IL 62225-5219

HQ USAF AFC4A 1
ATTN: SY
Scott Air Force Base, IL 62225-5421

HQ USAF Air Materiel Command 1
ATTN: AFMC/ENS
4375 Chidlaw Road, Suite 6
Wright-Patterson Air Force Base, OH 45433-5006

USAF Rome Laboratories/C3 1
ATTN: C3Y
Griffiss Air Force Base, NY 13441-5700

Other Organizations

HQ NASA 1
ATTN: Mr. Lynwood P. Randolph
300 "E" Street, SW
Washington, DC 20746

National Institute for Science and Technology 1
ATTN: ICST (Mr. Roger Martin)
Technology Building #225, Room B-266
Gaithersburg, MD 20899

National Institute for Science and Technology 1
Systems and Network Architecture Division
ATTN: ISE (Mr. Kevin Mills, Chief)
Technology Building #225, Room B-217
Gaithersburg, MD 20899

National Institute for Science and Technology 1
Systems and Network Architecture Division
ATTN: ISE (Mr. Gerald Mulvenna)
Technology Building #225, Room B-217
Gaithersburg, MD 20899

National Institute for Science and Technology 1
Network Protocols Section
ATTN: ISE (Mr. Richard Colella, Mr. Jim West)
Technology Building #225, Room B-217
Gaithersburg, MD 20899

National Institute for Science and Technology 1
ATTN: Mr. Fritz Schultz
Technology Building #225, Room B-266
Gaithersburg, MD 20899

National Institute for Science and Technology 1
ATTN: Leslie Collica
Technology Building #223, Room B-364
Gaithersburg, MD 20899

ARC Incorporated 1
ATTN: Steve Claiborne
234 S. Fraley Boulevard, Suite 308
Dumfries, VA 22026

ARC Defense Systems Division 1
ATTN: Mr. Mike Weber
670 Tinton Avenue
Tinton Falls, NJ 07724

Argonne National Laboratories 1
Division for Information Sciences
ATTN: A. Peter Campbell, Director
9700 South Cass Avenue, EID/900
Argonne, IL 60439-4832

AT&T Bell Laboratories 1
ATTN: Ms. Lorraine Kevra, Mr. Clyde Robicheaux
Routes 202/206 North, 5A210
Bedminster, NJ 07921

Battelle 1
Seattle Research Center
ATTN: C. Richard Schuller
4000 N. E. 41st Street
Seattle, WA 98105-5428

BDM Corporation 1
ATTN: Bill Walden, Charles Hayes,
W. E. Stewart
1501 BDM Way
McLean, Virginia 22102

BDM Corporation 1
ATTN: Mr. Jerry Dresser
BDMESC Victoria Plaza
Building 1, 615 Hope Road
Eatontown, NJ 07724

Booz Allen Hamilton, Inc. 1
ATTN: Elmer McDowell
4330 East-West Highway
Bethesda, MD 20814-4455

Center for Naval Analyses 1
401 Ford Avenue
P. O. Box 16268
Alexandria, VA 22302-0268

Computer and Business Equipment Manufacturer's Association 1
ATTN: ANSI X3 Secretariat
311 First Street, NW, Suite 500
Washington, DC 20001-2178

Computer Sciences Corporation 1
ATCCS Program Office
ATTN: Mr. Don Camp, Mr. Neil Vestermark
1301 Virginia Avenue, 4th Floor
Fort Washington, PA 19034

Computer Sciences Corporation 1
ATTN: Mr. Don Koppenhaver
788 Shrewsbury Avenue
Tinton Falls, NJ 07724

Digital Equipment Corporation 1
ATTN: Mr. Jim Isaak, Peter Smith
110 Spitbrook Road
Nashua, NH 03062

Digital Equipment Corporation 1
ATTN: Mr. Kevin Lewis
3020 Hamaker Court, Suite 100
Fairfax, VA 22031

Emerging Technologies Group, Inc. 1
ATTN: Mr. Harvey Hendin, Ms. Wendy Rauch
5 Kinsella Street
Dix Hills, NJ 11746

ITT Defense Communications Division 1
ATTN: David Blauvet
492 River Road
Nutley, NJ 07110-3696

Litton Data Systems 1
ATTN: Keith McNally
8000 Woodley Avenue
Van Nuys, CL 91409-7601

LOCE/BICES Project Office 2
ATTN: Richard H. Radcliffe, Jim Bain
Vector Data Systems
1150 S. Washington Street, Suite 300
Alexandria, VA 22314-4400

LOGICON 1
ATTN: E. Robert Sive, Darvel Stutts
145 Wyckoff Road, Suite 301
Eatontown, New Jersey 07724

LOGICON/Eagle Technologies, Inc. 1
ATTN: Dave Howe, Ray White
Systems Engineering Department
Linpro Park One, Suite 300
1831 Wiehle Avenue
Reston, VA 22090

LOGICON/Eagle Technologies, Inc. 1
ATTN: Fred Stuhrke
Systems Engineering Department
Linpro Park One, Suite 300
1831 Wiehle Avenue
Reston, VA 22090

LOGICON/Eagle Technologies, Inc. 1
ATTN: Judy Simpson, Erskin Sledd, Tom Blizzard
Systems Engineering Department
P. O. Box 1196
Dumfries, VA 22026-9196

Magnavox Corporation 1
ATTN: John Williams
1313 Production Road
Fort Wayne, Indiana 46808

Michigan State University 1
ATTN: Mr. Charles Severance
Computer Center, Room 301
E. Lansing, MI 48824

The MITRE Corporation 2
Tactical C3I
ATTN: Mr. William Blankhertz, Dr. Larry Dworkin
145 Wyckoff Road
Eatontown, NJ 07724

The MITRE Corporation 1
ATTN: Mr. Rene Dube, Jeff Hustad
Building 66157, Cushing Street
P. O. Box 925
Fort Huachuca, AZ 85613

The MITRE Corporation, Washington C3I 2
ATTN: Mr. Andrew Scholm
Mail Stop W 545
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mr. Dave Woodall, Mail Stop W 555
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mr. David C. Wood, Mail Stop W 643
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Ms. Gladys Reichlen, Mail Stop W 650
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mail Stop W545 (Mr. Larry Stine)
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mail Stop W956 (Mr. Robert Brown)
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Library Services, Mail Stop Z200
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Mr. Richard Kallagher
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation, Washington C3I 1
ATTN: Emily McCoy, Mail Stop W 725
7525 Colshire Drive
McLean, VA 22102-3481

The MITRE Corporation ATTN: Mr. Leo LaBarre, Mail Stop M245 Burlington Road Bedford, MA 01730	1
The MITRE Corporation ATTN: Mr. Paul J. Brusil Burlington Road Bedford, MA 01730	1
Open Software Foundation ATTN: Robert Hathaway 11 Cambridge Center Cambridge, MA 02142	1
SAIC Technology Services Company ATTN: Richard Halek 1001 Executive Drive Sierra Vista, AZ 85635	1
SPARTA, Inc. ATTN: Mr. Bob Harris, Charles Eldrige 7926 Jones Branch Road, Suite 900 McLean, VA 22102	1
State of Texas Department of Information Resources ATTN: Mr. Jerry L. Johnson Post Office Box 13564 Austin, TX 78711-3564	1
SWL Corporation ATTN: Phil Walker, Jim Mathwick 1900 Gallows Road Vienna, VA 22182	1
TELOS Federal Systems ATTN: Mr. Ernest Hamik 111 "C" Avenue Lawton, OK 73501	1
TRW Defense Systems Group ATTN: Mr. Hershie Krisch One Space Park Redondo Beach, CA 90278	1
X/OPEN 1750 Montgomery Street San Francisco, CA 94111	1
Defense Technical Information Center Cameron Station Alexandria, VA 22314	2
Institute for Defense Analyses 1801 N. Beauregard Street Alexandria, VA 22311-1772	40
TOTAL:	370

REFERENCES

REFERENCES

[AAP-4 1990] *NATO Standardization Agreements and Allied Publications*, AAP-4, 1990.

[AC/302 1990] *Report of AC/302(TSGCE) Meeting Held on 23-25 January 1990*, US Mission, NATO, 31 January 1990.

[ACCST 1986] *Air Command and Control System Master Plan (U)*, Volume IV, *Overall ACCS Design (U)*, Book 2, *Generic Portion (U)*, ACCST(86)282/057, NATO, April 1986, NATO CONFIDENTIAL.

[ACCST 1988] *Air Command and Control System Master Plan (U)*, Volume IV, *Overall ACCS Design Generic Portion (U)*, ACCST(86)281-282/057 (Revised)/ACC-1086, Supporting Document 4, *Structure and Characteristics of Organizational Components (U)*, May 1988, NATO CONFIDENTIAL.

[ACE 1988] *ACE Inventory of Key Tasks (U)*, December 1988, NATO CONFIDENTIAL.

[ACE ACCIS 1993] ACE ACCIS Target Architecture, Director General NACISA, September 1993, NATO UNCLASSIFIED.

[ACE ACCIS 1993a] *ACE ACCIS Implementation Strategy (AAIS)*, AC/317-D/60, NACISC, 30 June 1993, NATO UNCLASSIFIED.

[ACE ACCIS 1993b] ACE ACCIS Implementation Strategy (AAIS), NACISC, June 1993, NATO UNCLASSIFIED.

[ACE ACCIS 1993c] ACE ACCIS Implementation Strategy (AAIS), NACISC, June 1993, NATO UNCLASSIFIED.

[ACE ACCIS 1994a] *ACE ACCIS Core Capability and Capability Increments*, Draft for SHAPE Coordination, NACISC, 17 January 1994, NACISC, NATO UNCLASSIFIED.

[ACP 123 1991] *Final Draft ACP 123 Requirements Document*, Prepared by PRC, Incorporated, for the US Defense Information Systems Agency, Deliverable 6, 20 November 1991, UNCLASSIFIED.

[ACP 123 1991a] *ACP 123 Requirements Document*, Draft, 20 November 1993, ACP 123 Task Force, DCA (DISA), UNCLASSIFIED.

[ACP 167 1981] *Glossary of Communications-Electronics Terms*, ACP 167(F), NATO, August 1981.

[ACSA 1993] *Common Technical Interface Design Plan (CTIDP) Based on the Bilateral Interoperability Programs ADLER/AFATDS, AFATDS/BATES, and BATES/ADLER*, ASCA-012/00D, Artillery Systems Cooperation Activities (ASCA), 2 August 1993, NATO UNCLASSIFIED.

[Ada 9X 1990] *Ada 9X Project Report: Ada 9X Revision Issues*, Release 2, US Office of the Under Secretary of Defense for Acquisition, May 1990.

[ADatP-2 1985] *NATO Glossary of Automatic Data Processing (ADP) Terms and Definitions*, ADatP-2(D), December 1985, NATO UNCLASSIFIED.

[ADatP-3 1986] *NATO Message Text Formatting Systems*, Part IV, *Catalog of Standard Field Formats*, ADatP-3 (STANAG 5500), December 1986, NATO UNCLASSIFIED.

[ADatP-3 1986a] *NATO Message Text Formatting System*, Part 1, *System Concept and Description*, ADatP-3, Third Draft, 6 October 1986.

[ADatP-3 1993] *Automatic Data Processing (ADP) NATO Glossary (ADatP-3) Proposal List 45*, ISWG, NACISC, AC/317(WG/2)WP/86, 29 September 1993, NATO UNCLASSIFIED.

[ADS 1983] *Architectural Design Study (ADS) Final Report*, 3060/SHCOR/82, SHAPE, 10 January 1983, NATO UNCLASSIFIED.

[ADSIA 1986] *Transmission Independent Data Link Architecture*, ADSIA-RCA-C-10-86, 12 February 1986, NATO UNCLASSIFIED.

[ADSIA 1987] *The Need for Standardization of Data Management and Data Base Information Exchange in the NATO CCIS, Enclosure 2 to ADSIA-RCA-WP/44 (Revised), ADSIA*, September 1987, NATO UNCLASSIFIED.

[ADSIA 1988a] *Briefing to the 22nd ADSIA Plenary on the Quadrilateral Interoperability Program, Annex V to ADSIA-RCX-DS/22*, ADSIA Staff, 17-21 October 1988, NATO UNCLASSIFIED.

[ADSIA 1990] *Media Independent Data Link Architecture*, ADSIA-RCA-C-106-90, 28 May 1990, NATO UNCLASSIFIED.

[ADSIA 1993a] *Allied Data Systems Interoperability Agency (ADSIA)—An Introduction*, ADSIA, 26 January 1993, NATO UNCLASSIFIED.

[ADSIA 1993b] *Conceptual Message Data Model for NATO Land Force Command and Control (C2) Messages*, ADSIA(WG3)RDU-C-40-93, ADSIA Working Group 3, 8 September 1993, NATO UNCLASSIFIED.

[Ahern 1991] *Report of the US Representative (CAPT D. G. Ahern) to WG4*, June 1991, UNCLASSIFIED.

[AHWG 1990a] *Liaison to SG9 Concerning Work on the Quality of Service Issue*, TSGCE SG9 AHWG-OM, 27 June 1990, NATO UNCLASSIFIED.

[AHWG 1990b] SG9 AHWG-OSI Management Meeting Report, 25-29 June 1990, Ottawa, U.S. . .

[AHWG 1990] *NATO Requirements for Open Systems Management*, TSGCE SG9 AHWG-OM, 28 June 1990, NATO UNCLASSIFIED.

[AHWG-ISDN 1990] *Report of the 2nd Ad Hoc Meeting on ISDN, Paris, 24-26 April 1990*, AHWG on ISDN, May 1990, NATO UNCLASSIFIED.

[AHWG-OM 1989] *Response to Q62 on Quality of Service, Chair*, AHWG-OM, 10 March 1989.

[AHWG-OM 1990] Private Communication with the US Representative to the AHWG-OM, 19 June 1990, NATO UNCLASSIFIED.

[AHWG-S 1990] *Chairman's Report of the 8th Meeting, AC/302(TSGCE)SG/9 Ad Hoc Working Group on Security*, May 1990, NATO UNCLASSIFIED.

[AHWG-S 1990a] Private Communication with the Chair, TSGCE SG9 AHWG on Security, 18 June 1990, NATO UNCLASSIFIED.

[AIntP-3 1993] *Military Intelligence Data Management and Exchange Concept*, Allied Intelligence Publication Number 3 (AIntP-3), 9th Preliminary Draft, NATO Military Agency for Standardization (MAS), 23 September 1993, NATO UNCLASSIFIED.

[AJPO 1989] *Rationale for MIL-STD-1838A (CAIS)*, Prepared by SofTech, Inc., for the Ada Joint Program Office, 30 September 1989.

[AJPO 1992] *Available Ada Bindings*, Prepared by IIT Research Institute for Ada Joint Program Office, November 1992.

[Albarelli 1994] Private Communication from Mike Albarelli on ATCCS, OPEO CCS, UA Army CECOM, 18 January 1994, UNCLASSIFIED.

[Anderson 1989] *Windows and Widgets (MIT X), R. Anderson, Computer Systems Europe*, April 1989.

[Andrews 1990] *Towards an Australian Defence Organisation Integrated Communications Architecture*, Part 1, *Defence Science and Technology Organisation (DSTO)*, F. B. Andrews, et al., Electronics Research Laboratory Report ERL-0484-RE, April 1990, UNCLASSIFIED.

[Andrews 1993] "The Australian Defence Communications Corporate Plan and Its Underpinning Research Program," Brian Andrews and COL Gus Kollar, Defence Science & Technology Organization and Headquarters Australian Defence Force (Australia), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[ANSI 1991] *X3 Announces Solicitation of Comments on the Final Report of the Object-Oriented Database Task Group (OODBTG)*, ASC X3, Information Processing Systems News Release, 1 October 1991.

[ANSI 1991a] *X3T5 Meeting at CBEMA in Washington*, DC, 1-2 October 1991.

[ANSI 1993] *X3 Projects Manual X3/SD-4*, ANSI X3—Information Processing Systems, July 1993.

[ANSI Y14.26M 1989] *Digital Representation for Communication of Product Definition Data*, ANSI Y14.26M, Draft, 1989.

[APP 1991] *Application Portability Profile (APP): The US Government's Open System Environment Profile*, Systems and Software Technology Division, National Computer Systems Laboratory, National Institute of Standards and Technology, NIST Special Report, Public Review Draft, 15 November 1990, January 1991.

[APP 1992] *Application Portability Profile (APP): The US Government's Open System Environment Profile - OSE/1 Version*, Draft, Systems and Software Technology Division, National Computer Systems Laboratory, National Institute of Standards and Technology, NIST Special Report, Revised October 1992, 27 October 1992.

[APP 1993] *APP: Application Portability Profile: The US Government's Open System Environment Profile OSE/1*, Version 2.0, NIST Special Publication 500-210, Systems and Software

Technology Division, Computer Systems Laboratory, National Institute of Standards and Technology, June 1993.

[Army 1989] *US Army Transition Strategy*, HQ Department of the Army, 1989, UNCLASSIFIED.

[ASDC3I 1987] *Memorandum on Open Systems Interconnection Protocols*, ASD(C3I), 2 July 1987.

[ATCCIS 1988] *Architecture Definition*, ATCCIS Working Paper 24, Edition 2, 24 October 1988, NATO UNCLASSIFIED.

[ATCCIS 1990] *ATCCIS Phase II Final Report*, ATCCIS Permanent Working Group, SHAPE, October 1990, NATO RESTRICTED.

[ATCCIS 1991] *ATCCIS Phase III Project Brief*, ATCCIS Permanent Working Group, SHAPE, 22 November 1991, NATO UNCLASSIFIED.

[ATCCIS 1993] *ATCCIS Phase III Work Plan*, Edition 2.0, ATCCIS Permanent Working Group, SHAPE, 10 December 1993, NATO UNCLASSIFIED.

[ATCCIS WP 5-2 1993] *Battlefield Generic Hub*, Edition 1, ATCCIS Working Paper 5-2, April 1993, NATO UNCLASSIFIED.

[ATCCIS WP 5-2b 1993] *Fire Support Data Model*, Edition 1, ATCCIS Working Paper 5-2b, August 1993, NATO UNCLASSIFIED.

[ATCCIS WP 25 1988] *Technical Standards for the ATCCIS Architecture*, ATCCIS Working Paper 25, Edition 1.0, September 1988, NATO UNCLASSIFIED (IDA Memorandum Report M-519, September 1988, UNCLASSIFIED).

[ATCCIS WP 25 1990] *Technical Standards for CCISs*, ATCCIS Working Paper 25, Edition 2.0, August 1990, NATO UNCLASSIFIED (IDA Paper P-2459, August 1990, UNCLASSIFIED).

[ATCCIS WP 25 1992] *Technical Standards for CCISs*, ATCCIS Working Paper 25, Edition 3.0, NATO UNCLASSIFIED (IDA Paper P-2686, January 1992, UNCLASSIFIED).

[Bahnji 1990] *Transport Protocols and Internetworking in Low Bandwidth Tactical Networks*, Shiraz G. Bhanji, The MITRE Corporation, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Bailey 1990] "MOD(UK) Plans for OSI: Civil Section Relationship," M. A. Bailey, MOD(UK) Directorate General of Information Technology Systems (DGITS), *Proceedings of the SHAPE Technical Centre Military OSI Symposium*, 6-8 June 1990, NATO UNCLASSIFIED.

[Bainbridge 1989] *Report on JTC1 SC21/WG5 OSI Transaction Processing Rapporteur Group Meeting, Florence, 1-9 November 1989*, A. J. Bainbridge, British Standards Institute, IST/21:1850, 14 November 1989.

[Barlow Report] "An Update on CALS Implementation," *Barlow Report*, Volume 3, Issue 2.

[Baybrook 1990] "Integrated Geographic Information Systems (GISs) for Joint/Combined C3I Requirements," Thomas G. Baybrook and Tolbert A. Williams, Integraph Corporation, *Geo'89 Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[BBN 1989] *SIMNET Network and Protocols*, Report Number 7102, A. Pope, BBN Systems and Technology Corporation, July 1989.

[Beard 1993] *Letter to B. R. Gladman, Chairman TSGCE*, D. Blum and R. Rice, DS/ASG(93)159, Robin Beard, Assistant Secretary General for Defence Support, NATO, 25 May 1993, NATO UNCLASSIFIED.

[Beggs 1992] Private Communication with LTC Robert Beggs, Department of National Defence, Canada, 16 January 1992, NATO UNCLASSIFIED.

[Bevan 1989] "Briefing on ISO Standards for User System Interaction," N. Bevan, et al., *CHI'89 Conference*, May 1989.

[BICES 1988] *BICES User Requirements (U)*, Final Draft, 3 March 1988, CS/C/EL(88)259, AC/302(PG/7) Serial 25, NATO CONFIDENTIAL.

[BICES 1993] *STC, BPS, and ACE Data Modelling Activities*, David W. Lambert, Memorandum to BICES Team Leader, BT-M(93)181, 14 December 1993, NATO UNCLASSIFIED.

[BICES 1994] *Functional Area Analysis Interoperability*, David W. Lambert, BICES Team Draft Working Paper, BICES Team Office, IOPV1.2, 15 January 1994, NATO UNCLASSIFIED.

[Billingsley 1990] *The Standards Factor: Standards on the Horizon*, Pat Billingsley, SIGCHI Bulletin, Volume 22, Number 2, October 1990, pp. 10-12.

[Blankertz 1990] *Briefing to the Protocol Standards Steering Group on Tactical Data Networking In Europe*, Bill Blankertz, The MITRE Corporation, 27 February 1990.

[Bloom 1992] "STEP - Standard for the Exchange of Product Model Data," Howard M. Bloom, *CALS Journal*, Summer 1992, p. 80.

[Blum 1990] *Minimum Encoding Rules (MBER) for the Abstract Syntax Notation One (ASN.1)*, D. Blum and R. Rice, 4 April 1990.

[Bonatti 1993] "ASN.1 Enhancements to Support Tactical Data Communications," Chris D. Bonatti, Booz-Allen & Hamilton, Inc. (United States), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Booz-Allen 1991] *DoD Standardized Profiles*, Briefing to the DTMP by Booz-Allen-Hamilton, July 1991, UNCLASSIFIED.

[Borenstein 1991] "Multimedia Electronic Mail: Will the Dream Become a Reality?," Nathaniel S. Borenstein, *Communications of the ACM*, Volume 34, Number 4, April 1991, pp. 117-119.

[Bot 1993] "Communications Systems Network Interoperability (CNSI)—A Cooperative Project to Prove Feasibility of Network Interoperability Based on OSI Standards, Resulting in an International Demonstrator," Abraham Bot, TNO Physics and Electronics Laboratory (The Netherlands), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Boyer 1993] *PCIS and the Evolution of PCTE*, Michael F. Boyer, GEC-Marconi Software Systems, 1993.

[Bozman 1993] "Unix Brand Deal Approved," Jean S. Bozman, *Computerworld*, 11 October 1993, p. 4.

[Brettnacher 1988] "Accueil Logiciel Future: Overview of the Project," J. M. Brettnacher, et al., *ESPRIT '88—Putting the Technology to Use, Proceedings of the 5th Annual ESPRIT Conference*, Volume 1, 1988.

[Briggs 1988] *Briefing to ATCCIS PWG on SD&IC Plans*, John Briggs, ADSIA, 7 December 1988, NATO UNCLASSIFIED.

[Bruce 1992] *Designing Quality Databases with IDEF1X Information Models*, Thomas A. Bruce, Dorset House Publishing, 1992.

[Bryant 1993] "X.400 in the Tactical Environment—Results of Early Field Trials in the United States," LCdr Kathleen C. Bryant (USN), and LCdr David C. Chappell (USN), Defense Information Systems Agency (United States), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[BSI 1989] *Minutes of the IST21 Ad Hoc Security Meeting Held at the BSI Conference Centre*, BSI IST21, 11 December 1989.

[BSI 1991] *UK Comments on Progression of Security Frameworks in Open Systems*, BSI IST/21: 3049, 17 September 1991.

[Burgess 1992] "Novell to Buy Unix System from AT&T," John Burgess, *The Washington Post*, 22 December 1992, p. E-1.

[Burr 1991] *Security in ISDN*, William Burr, National Institute of Standards and Technology, NIST SP 500-189, September 1991, p. 31.

[C3 1989] *Implementation of Multicommand Required Operational Capability (MROC) 3-88, The Defense Mapping System (DMS)*, Director for C3 Systems, Joint Staff, 6 February 1989.

[CA 1989] *NATO Requirements for OSI Testing—Issues and Recommendations*, CA Contribution to NATO TSGCE SG9, 15 February 1989.

[CALS 1992] "CALS Testing: Programs, Status and Strategy," Sharon Kemmerer, *CALS Journal*, Summer 1992, p. 57.

[CALS 1993] "The CALS Program Update," *CALS Journal*, Fall 1993, p. 15.

[CALS/CE 1992] "Standards Briefs," *CALS/CE Report*, Volume 5, Number 2, February 1992, p. 14.

[CALS/CE 1992a] *CALS Information Services from NTIS*, CALS/CE Information Center, 1992.

[Cardonna 1988] *Briefing to TSGCE SG9 on Conformance Testing*, Ralph Cardonna, US Precoordination Meeting, 30 August 1988.

[Cargill 1989] *Information Technology Standardization: Theory, Process, and Organizations*, Carl F. Cargill, Digital Press, Bedford, Massachusetts, 1989.

[Carlson 1991] "A Survey of Computer Graphics Image Encoding and Storage Formats," Wayne E. Carlson, *Computer Graphics*, Volume 25, Number 2, April 1991, pp. 67-75.

[Cassese 1990] "Secure Data Communication Defence System," Vincenzo Cassese, Alcatel CIT, France, *Proceedings of the SHAPE Technical Centre Military OSI Symposium*, 6-8 June 1990, NATO UNCLASSIFIED.

[CBEMA 1989] *X-3 Information Processing Systems Accredited Standards Committee Projects Manual*, X3/SD-4, CBEMA, 1989.

[CCTA 1990] *UK Government OSI Profile*, Volume I, *Introduction*, Version 3.1, Central Computer and Telecommunications Agency, London, 1990.

[CCTA 1990a] *UK Government OSI Profile*, Volume II, *Specification*, Version 3.1, Central Computer and Telecommunications Agency, London, 1990.

[CCTA 1990b] *UK Government OSI Profile*, Volume III, *Procurement Handbook*, Version 3.1, Central Computer and Telecommunications Agency, London, 1990.

[CCTA 1991] *Towards Open Systems: The CCTA "Migration to OSI" Programme*, IS Notice Number 27, CCTA, 6 September 1991.

[CCTA 1991a] *Electronic Data Interchange*, IS Notice Number 31, Central Computer and Telecommunications Agency, United Kingdom, 25 November 1991.

[CCTA 1992a] *GOSIP 4 Supplier Set*, Six volumes: Volume 1, *Overview;* Volume 2, *Network Support*, Volume 3, *Application Services (1);* Volume 4, *Application Services (2);* Volume 5, *Interchange Formats and Ancillary Services;* and Volume 6, *Annexes* (containing interim specifications), 1992.

[CCTA 1992b] *UK Government OSI Profile, GOSIP 4, Procurement Handbook*, Fourth Edition, Five volumes: Volume 1, *Overview;* Volume 2, *Network Support;* Volume 3, *Application Services;* Volume 4, *Information Interchange and Supporting Services;* Volume 5, *Annexes* (containing tutorial material and references), 1992.

[CEC 1988] *The Value and Use of IT Standards in Public Procurement*, PPSC-IT N268.1, Commission of the European Communities, August 1988.

[CECOM 1989] Discussions with Staff from the Information Systems Directorate, CECOM, March 1989.

[CEN 1989] *Result of Formal Vote on prENV 40002*, CEN, 22 November 1989.

[Cerny 1991] "Fiber-Optic and Copper LANs," Richard Cerny, *Handbook of Local Area Networks*, John P. Slone and Ann Drinan, Editors, Auerbach Publishers, 1991.

[CFS 1993] "Federal Criteria for Information Technology Security," *Information Processing Standards Newsletter*, Center for Standards, Defense Information Systems Agency, Number 93-1, February 1993.

[CFS 1993a] "MIL-STD-SDD Harmonization," *Information Processing Standards Newsletter*, Center for Standards, Defense Information Systems Agency, Number 93-1, February 1993.

[CFS 1993b] "POSIX Activities," *Information Processing Standards Newsletter*, Center for Standards, Defense Information Systems Agency, Number 93-1, February 1993.

[CFS 1993c] "Object Information Management," *Information Processing Standards Newsletter*, Center for Standards, Defense Information Systems Agency, Number 93-1, February 1993.

[CGA 1992] "Standards Report," *TechInfo*, Computer Graphics Association (CGA), July 1992, pp. 3-4.

[Chair 1989] Private Communication with the Chair, TSGCE SG9 WG1, 14 March 1989.

[Chesson 1988] *XTP/PE Overview*, Greg Chesson, Silicon Graphics, April 1988.

[Christiansen 1993] "Practical Issues in NATO Network Management," Brian Christiansen, SHAPE Technical Centre (The Netherlands), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[CIM 1991] *Technical Reference Model for Corporate Information Management*, Versions 1.0, Center for Information Management, US Defense Information Systems Agency, 4 November 1991, UNCLASSIFIED.

[CIM TRM 1992] *DoD Technical Architecture Framework for Information Management*, Volume 3, *DoD Technical Reference Model for Information Management*, Version 1.1, 2 October 1992.

[CIS 1990] *CASE Interface Services Base Document*, CASE Integration Services (CIS) Committee, September 1990.

[Claasen 1994] Private Communication from Walter Claasen on WP 25 Comments, DISA/JIEO, 18 February 1994, UNCLASSIFIED.

[Clifford 1988] "The Development of PEX—A Graphics Extension to X11," W. H. Clifford, et al., *EUROGRAPHICS '88, Proceedings of the European Computer Graphics Conference and Exhibition*, Nice, France, 12-16 September, 1988.

[CNAD 1992] *Naming and Addressing*, DS/ASG(92)17, P. Merrill, Permanent Chairman CNAD, January 1992, NATO UNCLASSIFIED.

[CODASYL 1980] *A Framework for Distributed Database Systems: Distribution Alternatives and Generic Architecture*, CODASYL, 1980.

[COE 1991] *Fleet Communications in the Copernicus Architecture*, Final Draft, 20 June 1991, UNCLASSIFIED.

[Collela 1992] Private Communication with Richard Collela, NIST, 14 January 1992, UNCLASSIFIED.

[Collela 1992a] *Work Plan for the Development of a Common OSI Specification*, Private Communication from Richard Collela, NIST, 14 January 1992, UNCLASSIFIED.

[Computerworld 1991] "ISDN Not Popular in Europe - Yet," *Computerworld*, November 25, 1991, p. 45.

[COPERNICUS 1991] *Fleet Communications in the Copernicus Architecture*, Final Draft, 20 June 1991, UNCLASSIFIED.

[COS 1989] *Cooperation Agreement with Japan*, Memorandum for the Members of the COS Board of Trustees, Corporation for Open Systems, 19 June 1989.

[CSC 1985] *Computer Security Requirements—Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (Yellow Book)*, CSC-STD-003-85, DoD Computer Security Center, June 1985.

[CSC 1985a] *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements—Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments (Yellow Book Rationale)*, CSC-STD-004-85, DoD Computer Security Center, June 1985.

[CSC 1985b] *Department of Defense Trusted Computer System Evaluation Criteria* (Orange Book), DoD 5200.28-STD, DoD Computer Security Center, December 1985.

[CSC 1987] *Trusted Network Interpretation (Red Book)*, NCSG-TG-005, Version 1, National Computer Security Center, July 1987.

[CSI 1990] "Standardization Activities," *Computer Standards and Interfaces*, Volume 11, Number 1, 1990, p. 78.

[CSL 1992] *CSL Bulletin*, National Institute of Standards and Technology, Computer Systems Laboratory (CSL), December 1992.

[Cugini 1992] "Computer Graphics Testing," John Cugini, *NIST User's Forum on APP and OSE*, 14 May 1992.

[Curcio 1994] Private Communication with Frank Curcio, DISA/JIEO, February 1994.

[DAFTG 1982] *An Architectural Framework for Database Standardization*, Draft, ANSI DAFTG, 1982.

[Davidson 1991] *Guide to SONET*, Robert P. Davidson and Nathan J. Muller, Telecom Library, 1991.

[Davis 1990] "Relationship Between ECMA PCTE and PCTE+," Hugh Davis, *PCTE Newsletter*, Number 4, June 1990, P. 12.

[Davis 1992] *PCTE Overview*, Hugh Davis, NIST ISEE Users' Forum, 9 November 1992.

[DCA 1988] *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy*, Defense Communications System Organization, DCA, May 1988 (promulgated 17 June 1988).

[DCA 1988a] *Defense Message System (DMS) Target Architecture and Implementation Strategy (TAIS)*, DCA, December 1988.

[DCA 1989] *WWMCCS ADP Modernization (WAM) Decision Coordinating Paper (DCP)*, Joint Data Systems Support Center, Defense Communications Agency, November 1989.

[DCA 1989a] *Briefing on OSI Security Standards, Goals of NIST*, Briefing to the Protocol Standards Steering Group, DCA/NSA/NIST, 31 January 1989.

[DCA 1989b] *BFE Interface Control Document, BLACKER Program Office*, US Defense Communications Agency, 21 March 1989.

[DCA 1989c] *Briefing to the US Postcoordination Meeting for TSGCE SG9 on Defense Message System*, DCA, 21 March 1989.

[DCA 1990] *Briefing on BLACKER*, INCA Project Office, US Defense Communications Agency, May 1990.

[DCCP 1991] *Defence Communications Corporate Plan 1991-2001*, AGPS, Department of Defence, Canberra, Australia, Mary 1991.

[DDI 1992] *Open Systems Implementation and the Technical Reference Model*, Policy Memorandum, Director of Defense Information, 12 February 1992, UNCLASSIFIED.

[Dempsey 1990] *The Multidriver: A Reliable Multicast Service Using the Xpress Transfer Protocol*, S. J. Dempsey, J. C, Fenton, and A. C. Weaver, 15th Conference on Local Computer Networks, Minneapolis, Minnesota, October 1990.

[Deutch 1987] *Database Management System Standards, Report of Past Progress and Future Prospects,* Donald R. Deutch, G. E. Information Services, US National Institute of Standards and Technology Symposium, 3 December 1987.

[DGNACISA 1992] *Protocol Standardization for Secure Computer-to-Computer Data Transfer,* APD/CSDB(92)02D, Director General NACISA, 14 January 1992.

[DGSA 1993] *Department of Defense Goal Security Architecture (DGSA),* Center for Information System Security Defense Information System Security Program, Version 1.0, 1 August 1993.

[Di Pasquale 1993] "Standardization of Inter-System Radio Transmissions on the Battlefield," Sylvie Ghez Di Pasquale, Isabelle Petry, and B. Vinson Rouchon, Thompson-CFS/RGS and French Ministry of Defence (France), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993,* STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Dibble 1990] "UK Defence Packet Switched Network (DPSN)," Alan Dibble, DSLC, and John Laws, RSRE, UK MOD, *Proceedings of the SHAPE Technical Centre Military OSI Symposium,* 6-8 June 1990, NATO UNCLASSIFIED.

[DIS 8824 1986] *Information Processing Systems - Open Systems Interconnection, Specification of Abstract Syntax Notation One* (ASN.1), ISO/DIS 8824, 1986.

[DIS 8825 1986] *Information Processing Systems - Open Systems Interconnection, Specification of Basic Encoding Rules for Abstract Syntax Notation One* (ASN.1), ISO/DIS 8825, 1986.

[DISA 1990] *X12/DISA Information Manual,* Data Interchange Standards Association (DISA), Incorporated (ANSI X12 Secretariat), Spring 1990.

[DISA 1991] *Defense Message System Required Operational Messaging Characteristics,* Draft, DISA, 1 November 1991, UNCLASSIFIED.

[DISA/CIM 1992] *Business Process Improvement Modelling Underway,* Briefing on Business Process Improvement, DISA/CIM, 23 April 1992.

[DISC 1993a] "Electronic Data Interchange—Time for Rationalization," *DISC Newsletter,* British Standards Institute, Issue 4, July 1993.

[DISC 1993b] *A Comparison of PCTE and IRDS Standards: Project 073/0010 (1052),* British Standards Institute, December 1993.

[DISC4 1988] *Army Data Management and Standards Program,* AR 25-9, Office of the Secretary of the Army, Director of Information Systems for Command, Control, Communications, and Computers (DISC4), July 1988, UNCLASSIFIED.

[DISSP 1991] *Defense-Wide Information Systems Security Program (DISSP),* JTC3A Architecture Review, National Security Agency (Dave Stephan), 19 September 1991, UNCLASSIFIED.

[DK MOD 1994] Private Communication from Denmark Ministry of Defense on CCISs, 11 February 1994, NATO UNCLASSIFIED.

[DMA c1990] *DMA Standardization,* Defense Mapping Agency, Data Information Sheet, n.d.

[DoD 1976] *Development and Use of Non-Government Specifications and Standards,* Department of Defense Instruction 4120.20, Department of Defense, 1976.

[DoD 7920.2 1990] *Automated Information System (AIS) Life-Cycle Management Review and Milestone Approval Procedures,* US Department of Defense Directive 7920.2, US Department of Defense, 7 March 1990.

[DoD 8320.1-M 1993] *Data Administration Procedures,* DoD 8320.1-M, Draft, ASD(C3I), 23 September 1993.

[DoD HCI Style Guide 1992] *DoD Human-Computer Interface (HCI) Style Guide,* Draft, DISA, 1992, UNCLASSIFIED (see TAFIM).

[DODIIS 1993] *DODIIS Profile of the DoD Technical Reference Model for Information Management,* US DoD Intelligence Information System (DODIIS) Management Board, June 1993, UNCLASSIFIED.

[DoD Instruction 8020.1 1992] *Functional Process Improvement Program,* Draft, DoD Instruction 8020.1, ASD(C3I), 1 October 1992, UNCLASSIFIED.

[Dowling 1988] "Second PCTE+ International Review," E. J. Dowling, *Ada User,* Volume 9, Number 3, 1988.

[DRA 1994] Private Communication from the Defence Research Establishment, Fort Halstead, UK MOD, 28 January 1994, UNCLASSIFIED.

[DSPO 1991] *Digital Representation for Communication of Product Data: IGES Application Subsets; and MIL-D-28003, Digital Representation for Communication of Illustration Data: CGM Application Profile,* DoD Memorandum on Coordination of Proposed Revisions A to MIL-D-28000, DoD Defense Systems and Programs Office, Alexandria, VA, April 4, 1991.

[DTMP 1993a] *Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) Meeting, 28-29 January 1993,* Richard McLane, Chair DTMP, DISA/JIEO/TBBD, 20 February 1993, UNCLASSIFIED.

[DTMP 1993b] *Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) Meeting, 22-23 April 1993,* Richard McLane, Chair DTMP, DISA/JIEO/TBBD, 23 June 1993, UNCLASSIFIED.

[DTMP 1993c] *Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) Meeting, 22-23 July 1993,* Richard McLane, Chair DTMP, DISA/JIEO/TBBD, 23 August 1993, UNCLASSIFIED.

[DTMP 1993d] *Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) Meeting, 28-29 October 1993,* Richard McLane, Chair DTMP, DISA/JIEO/TBBD, 2 December 1993, UNCLASSIFIED.

[DTMP 1994a] *Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) Meeting, 27-28 January 1994,* Richard McLane, Chair DTMP, DISA/JIEO/TBBD, February 1994, UNCLASSIFIED.

[ECMA 1985] *ECMA-DB Remote Database Access Service and Protocol,* Final Draft, European Computer Manufacturers Association, 1985.

[ECMA 1987] *Framework for OSI Management,* TR/37, European Computer Manufacturers Association, January 1987.

[ECMA 1988] *Security in Open Systems—A Security Framework,* ECMA TR/46, European Computer Manufacturers Association, July 1988.

[Edelstein 1991] "Internationalizing Software Engineering Standards," D. Vera Edelstein, Roger Fujii, Craig Guerdat, and Pasquale Sullo, *IEEE Computer,* March 1991, pp. 74-78.

[ESC 1993] *ESC Software Standards,* Memorandum from Gordon E. Fornell, Department of the Air Force, HQ Electronic Systems Center (AFMC), Hanscom Air Force Base, MA 10731, 6 April 1993.

[ETG 30 1993] *EWOS Technical Guide on EDI,* ETG 30, EWOS, September 1993.

[EUROCOM D/1] *EUROCOM Tactical Communications Systems,* Basic Parameters (D/1), September 1986.

[EWOS 1990] *File Transfer Access and Management - FTAM Remote Actions (RA), Service and Protocol,* EWOS/ETG003, EWOS/EG FT, January 1990.

[EWOS 1990a] *Draft Functional Profile A/3311, Common Facilities—MTA to MTA,* Working Draft on the Message Handling System, Version 9.2, *European Workshop for Open Systems (EWOS),* May 1990.

[EWOS 1991] *Draft Taxonomy for Distributed Transaction Processing,* EWOS/EGTP/91/12; EWOS/TA/91/14, 13 February 1991, DRAFT.

[EWOS 1991a] *Management Information Catalogue,* Sixth Draft, EWOS/EG/NM/91/115, September 1991.

[EWOS TA/93/331 1993] *Proposal for EWOS EG EDI,* Chairperson EWOS Ad Hoc Group on EDI, October 1993.

[EWOS TA/93/355 1993] *Proposed New Work Item for EG NM,* ISO/Internet Management Coexistence Process, November 1993.

[Favreau 1990] *US Testing Program: Moving Toward GOSIP Version 2.0,* Jean-Philippe Favreau and J. Stephen Nightingale, NIST Users' Forum on APP and OSE, NIST, 14 May 1992.

[Favreau 1992] *The US GOSIP Testing Program,* Jean-Philippe Favreau, Kevin L. Mills, and J. Stephen Nightingale, NIST, 31 July 1990.

[FGAN 1994] Private Communication from K. Wagner on HEROS, FGAN (GE MOD), 12 February 1994, NATO UNCLASSIFIED.

[FIPS 183 1993] *Integration Definition for Function Modeling (IDEF0),* US Department of Commerce, December 1993.

[FIPS 184 1993] *Integration Definition for Information Modeling (IDEF1X),* US Department of Commerce, December 1993.

[FIRP 1994] *FIRP Draft Report,* US Federal Internetworking Requirements Panel, January 1994.

[Fisher 1991] *APP Update,* Gary E. Fisher, APP/OSE Users' Forum, NIST, 9 May 1991.

[Fisher 1992] *Application Portability Profile: Version 2 Update,* Gary E. Fisher, NIST Users' Forum on APP and OSE, NIST, November 10, 1992.

[Ford 1987] *Quadrilateral Mapping Schema, Maneuver Control System, CSD-TR2529,* Ford Aerospace and Communications Company for US Army Communications-Electronics Command, 25 September 1987.

[Fowler 1993] "RA90—The Future Bearer Service Network of the French Air Force," Max, Fowler and Bryan Adderley, EDS-Scicon Defence and Army CIS Agency, MOD (United Kingdom),

Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Fox 1991] "Standards and the Emergence of Digital Multimedia Systems," Edward A. Fox, *Communications of the ACM*, Volume 34, Number 4, April 1991, pp. 26-29.

[FR MOD 1994] Private Communication from French Ministry of Defense on CCISs, 25 February 1994, NATO UNCLASSIFIED.

[France 1989] *Commentaries on the STANAGs of WG1*, Contribution by France to TSGCE SG9/WG1, February 1989, NATO UNCLASSIFIED.

[Frantz 1992] "FIMS: Form Interface Management System," Dan Frantz, *Open Systems Tracking Report*, Volume 1, Number 4, July 1992, p. 4.

[Freeman 1991] Private Communication with Murray Freeman, Secretary of X3T2, 12 June 1991.

[G-LOTOS 1988] *G-LOTOS: A Graphical Syntax for LOTOS*, Attachment to SC21 N 3253, December 1988.

[Galitzer 1991] *Measuring GOSIP's Appropriateness for the Tactical User*, Briefing, S. Galitzer, MITRE, 10 April 1991, UNCLASSIFIED.

[Gallagher 1988] Discussions with Lynn Gallagher, Institute for Computer Sciences and Technology, US National Institute of Standards and Technology, Gaithersburg, MD, 24 May 1988.

[Gallagher 1990] *SQL3 Support for CALS Applications*, Leonard Gallagher, NIST, 21 December 1990.

[Gallagher 1991] *Memo to SC21 TAG Regarding ISO/IEC Projects on SQL and RDA Actions Taken at May/June 1991 SC21/WG3 Meetings in Arles, France*, Leonard Gallagher, 1991.

[Gallagher 1991a] *Database Management Standards: Status and Applicability*, Leonard Gallagher, NIST, 11 July 1991.

[GAM 1987] *Military Real Time Local Area Network*, GAM-T-103, Ministre de la Defense, Republique Francaise, 9 February 1987.

[Gambrel 1991] "Profiles," B. Gambrel, UNISYS, *8th APP/OSE Workshop*, NIST, Gaithersburg, MD, 12 November 1991.

[Gardner 1993] "Use of OSI Directory for Military Messaging," Gardner, Ella, and Emily McCoy, MITRE (United States), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Gee 1991] *Report of the US Representative (Sherman Gee) on SG9/WG3*, 18 October 1991, UNCLASSIFIED.

[Genesereth 1992] *Knowledge Interchange Format (KIF) Version 3.0 Reference Manual*, Michael R. Genesereth and Richard E. Fikes, Logic Group Report Logic-92-1, Computer Science Department, Stanford University, June 1992.

[Geo 1992] "Update," *Geo Information Systems*, October 1992, p. 70.

[German 1993] "ISDN-Communications Network for the German Armed Forces," D. A. German and T. K. Grant, Computing Devices Canada and Protocol Standards Communications, Inc. (Canada), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Gladman 1993] *A New Structure and Organisation for the NATO Tri-Service Group on Communications and Electronics (TSGCE)*, Letter to Representatives and Supporting Staff of TSGCE, D/DCIS(Eng)6-163, Dr. Brian R. Gladman, Chairman TSGCE, 24 June 1993, NATO UNCLASSIFIED.

[Goldfine 1988] *A Technical Overview of the Information Resource Dictionary*, NBSIR 86-3700, Alan Goldfine and Patricia Konig, US National Institute of Standards and Technology, January 1988.

[Goldfine 1991] Private Communication with Alan Goldfine, NIST, 18 April 1991.

[Goldon 1994] *CNAD/TSGCE Restructuring*, 4th Revision, Goldon, TSGCE Chairman, 17 January 1994, UNCLASSIFIED.

[GOSIP 1988] *Government Open Systems Interconnection Profile (GOSIP)*, FIPS 146, Version 1, US National Institute of Standards and Technology, 15 August 1988.

[GOSIP 1990] *US Government Open Systems Interconnection Profile (GOSIP)*, Version 2.0, Federal Information Processing Standard (FIPS) 146-1, October 1990, DRAFT.

[Goulde 1993] "Tomorrow's Microkernel-Based Unix Operating Systems," *Open Information Systems*, Volume 8, Number 8, August 1993.

[Government Computing 1993] "MOD Sets New Security Standards," *Government Computing*, Volume 7, Number 1, GC Magazine and Exhibitions, Limited (UK), October/November 1993.

[Greco 1988] "Windowing Systems Overview," F. D. Greco, *Program Journal*, Volume 6, Number 4, July-August 1988.

[Griefenstein 1989] *Briefing on EUROPE 92—The European Community's Approach to Integration in the Information Technology Area*, Fred Griefenstein, Softsiel Corporation, San Diego, 15 May 1989.

[Gungor 1993] "Evolutionary Architectural Framework for Distributed Information Systems," Ismet Gungor, SHAPE (Belgium), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Gutman 1990] *Report on the SG/9 AHWG-OSI Management Meeting Held in San Diego During 5-9 February 1990*, US Representative (Lew Gutman), 13 February 1990.

[Haak 1993] "Implementation of an X.400 Message Store," Norbert Haak, and Reinhard Detering, FGAN (Germany), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Haber 1991] "New Image Buzzwords: JPEG and JBIG," Lynn Haber, *Network World*, Volume 8, Number 7, February 18, 1991, pp. 41 and 55.

[Hall 1991] "Conformance Testing for FIPS 151-1 (POSIX)," James Hall, *7th OSE/APP Users' Forum*, May 9, 1991 NIST, Gaithersburg, MD.

[Hankinson 1988] *Briefing on Applications Software Portability*, Allen L. Hankinson, Institute for Computer Sciences and Technology, US National Institute of Standards and Technology, Gaithersburg, MD, 1988.

[Hankinson 1991] "APP Update," Al Hankinson, *APP/OSE Users' Forum*, NIST, Gaithersburg, MD, 9 May 1991.

[Harris 1991] *Software Product Specification for the DoD Connectionless-Mode Network Protocol*, Final Draft, Robert T. Harris, SPARTA, Inc., for the Defense Communications Engineering Center of the Defense Information Systems Agency, 11 March 1991, UNCLASSIFIED.

[Hartley 190] *ISDN Journal*, D. Hartley, University of Cambridge Computer Laboratory, November 1990.

[HDTV 1993] "Alliance Sets HDTV Tech Specs," *Washington Technology*, November 4, 1993.

[Hind 1993] "The Integration of SATCOM into Networks Using OSI and ISDN Standards," Ray Hind, SHAPE Technical Center (The Netherlands), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Hovey 1992] "OSI Implementors Workshop," Richard Hovey, *Open Systems Standards Tracking Report*, Volume 1, Number 2, January 1992, p. 3.

[Howe 1991] *Report of AC/302 Tri-Service Group on Communications and Electronic Equipment (TSGCE) Meeting of 16-17 September 1991*, US Representative to TSGCE (Mr. Howe), 7 October 1991, NATO UNCLASSIFIED.

[Humphreys 1991] *Security Features in International Standardized Profiles (ISPs)*, Discussion Document by E. J. Humphreys, Chair of IST33, 31 January 1991, distributed as IST/21 N 2652, 14 March 1991.

[Hunt 1994] Private Communication with CDR Tony Hunt (MOD-UK), SHAPE Policy and Requirements Division (C2 Requirements Section), 25 January 1994.

[Hurd 1993] "Motif," *Open Systems Standards Tracking Report*, Volume 2, Number 5, October 1993, pp. 3-4. .

[IDA 1991] *A Preliminary Description of a Target Architecture for Generic Command and Control Information Systems*, IDA Paper P-2490, Draft, Institute for Defense Analyses, August 1991.

[IDA 1992] *Proposed Modifications for Next Edition of ATCCIS WP 25 and Technical Standards for CCISs*, IDA Document D-1205, Institute for Defense Analyses, August 1992.

[IEEE 1983] *Software Engineering Standards, Institute of Electrical and Electronics Engineers*, Third Edition, 1983, Second Printing October 1989.

[IEEE 1991] "IEEE TCOS Standards Status," *POSIX Tracking Report*, Volume 3, Issue 3, July 1991, p. 3.

[IEEE 1992] *Draft Guide to the POSIX Open System Environment*, P1003.0/D15, Technical Committee on Operating Systems and Application Environments of the IEEE Computer Society, June 1992.

[IEEE 1993] *Draft Guide to the POSIX Open System Environment*, P1003.0/D16, Technical Committee on Operating Systems and Application Environments of the IEEE Computer Society, October 1993.

[IEEE SILS 1993] *IEEE Standard for Interoperable LAN/MAN Security (SILS), Clause 3—Key Management Protocol*, IEEE 802.10 Committee, 12 September 1993.

[IGES 1986] *Initial Graphics Exchange Specification, Version 3.0*, ANSI DP ANS Y14.26M, 1986.

[IGOSS 1993] *The Industry/Government Open Systems Specification*, Draft, US and Canadian Governments, MAP and Top User Groups, EPRI, January 1993, UNCLASSIFIED.

[IMA 1991] *The Army Long Range Plan for the Information Mission Area (IMA)*, Office of the Director of Information Systems for Command, Control, Communications and Computers, 11 January 1991.

[INI 1987] *The MAP Book: An Introduction to Industrial Networking*, Industrial Networking Incorporated, 1987.

[IRDS 1993] *IRDS Services Architecture Technical Report*, USA National Body 27 January 1993.

[ISO 1993] *ISO Catalogue*, International Organization for Standardization, Geneva, 1993.

[ISO 9545/PDAM 1 1991] *Information Technology - Open Systems Interconnection - Application Layer Structure - Proposed Draft Amendment 1: Extended Application Layer Structure*, ISO/IEC 9545/PDAM 1, 15 April 1991.

[IST/21 1534 1988] *Technical Report—Tutorial for Reference Model of Data Management*, Project Description for Project JTC1.21.30.2, IST/21 1534 (WG3 N 572), SC21/WG3, March 1988.

[IST/21: 2499 1991] *Report on the Anaheim IRDS Meetings*, IST/21: 2499, 18 January 1991.

[IST/21: 2525 1991] *IST/21 Project File*, January 1991, 30 January 1991.

[IST/21: 2852 1991] *POSIX Security Call for New Work Items*, SC22/WG15, IST/21:2852, June 1991.

[IST/21:1721 1989] *Notes on IST21 Ad Hoc Meeting on Distributed Applications*, IST/21:1721, British Standards Institute IST21, 25 July 1989.

[IST/21:1868 1989] *Functional Standards for the X.500 Directory*, IST/21:1868, IST21/4/DIR, British Standards Institute, 4 October 1989.

[IST/21:2041 1990] *Report of Joint ISO/IEC JTC1 SC21/WG4 and CCITT SG VIII(Q20) Meeting on Enhancements to the Directory, Geneva, February 5th to 14th 1990*, IST/21:2041, British Standards Institute IST21, 19 March 1990.

[IST/21:2160 1990] *Report on SC21 Plenary, Held in Seoul, 5-6 June 1990*, IST/21:2160, July 1990.

[IST/21:2170 1990] *JTC1 Workshop on Security*, London, 5-7 November 1990, IST/21:2170, British Standards Institute IST21, 29 June 1990.

[IST21:4803 1994] *IST/21 Project File January 1994*, Technical Committee IST/21, Open Systems Interconnection, Data Management, and Open Distributed Processing, British Standards Institute, 11 January 1994 (excerpts provided by DRA-Fort Halstead).

[ISWG 1991] *NATO Data Management Policy*, Working Paper, AC/317(WG/2)WP/67, ISWG, 28 August 1991, NATO UNCLASSIFIED.

[ITSEC 1990] *Information Technology Security Evaluation Criteria (ITSEC)—Harmonised Criteria of France, Germany, The Netherlands, and the United Kingdom*, Draft, Version 1, 2 May 1990.

[ITSTC 1989] *Study and Investigation Mandate for OSI Conformance Testing Methodology*, ITSTC N 1048, CEN/CENELEC Information Technology Steering Committee, 28 July 1989.

[ITU-TS I.121 1990] *Broadband Aspects of ISDN*, ITU-TS Recommendation I.121, 1990.

[J6J 1991] *Command, Control, Communications, Computers, and Intelligence (C4I) for the Warrior*, Draft, Joint Staff J6J, 17 October 1991, UNCLASSIFIED.

[JIEO MIL-STD-xxx 1992] *Military Standard Open Systems Environment (OSE) Profile for Imminent Acquisitions, MIL-STD-xxx*, 18 November 1992, Draft 3.

[Johnson 1994] Private Communication from Jerry Johnson on OIW TC-OSE, February 1994.

[JTAP 1991] *Standards Necessary to Define Interfaces for Applications Portability (IAP)*, Final Report, April 1991 [JTC1 N 1335].

[JTC1 N 1011 1990] *Results of National Body Survey*, JTC1 N 1011, 10 October 1990.

[JTC1 N 1161 1991] *Report of the Meeting of the Ad Hoc Technical Study Group on Multimedia and Hypermedia Held 12-14 December 1990*, New York, NY, ISO/IEC JTC1 N 1161, 8 January 1991.

[JTC1 N 1485 1991] *Final Disposition of Proposal for a New Work Item on RDA Support for Stored SBL Statements*, JTC1 N 1485, 16 August 1991.

[JTC1 N 1763 1992] *CCITT Circular Number 18 Regarding the Catalogue of CCITT Recommendations*, T. Irmer, Director of the CCITT, JTC1 N 1763, 6 January 1992.

[JTC1 N 2775 1993] *Summary of Voting on Document JTC1 N 2621, Proposal for a New Work Item: Conceptual Schema Modelling Facility*, December 1993.

[JTFS 92-468 1992] *Head of Delegation Report to JTC1 TAG Authorized Subgroup Meeting of JTC1 Special Group on Functional Standardization, London, UK, December 8-11, 1992*, Clyde S. Robichaux, 18 December 1992.

[Jurgen 1992] "An Abundance of Video Formats," Ronald K. Jurgen, *IEEE Spectrum*, March 1992, pp. 27-28.

[Keane 1991] *CIM Terminology*, Private Communication from Mr. John Keane, US DoD CIM Standards Office, CIM/XI, 16 July 1991, UNCLASSIFIED.

[Kemp 1990] Facsimile Communication from Alstair Kemp, IEE, London, 10 July 1990.

[Kennedy 1989] "Management Requirements Arising from a NATO Study of Quality of Service," Paul Kennedy, Chris Sluman, and Peter Pranschke, *Integrated Network Management*, B. Meandzija and J. Westcott (Editors), Elsevier Science Publishers B.V., The Netherlands, 1989 (pp. 133-140).

[Kenworthy 1991] Private Communication with William Kenworthy, Chair ANSI X3L8, (703) 693-8174, 16 May 1991.

[Kernighan 1988] *The C Programming Language*, Brian W. Kernighan and Dennis M. Ritchie, Second Edition, Prentice Hall, 1988.

[Kind 1993] *Army Tactical Command and Control Information System (ATCCIS) Study*, Memorandum for the Supreme Allied Commander, Europe (SACEUR), SHAPE, LtGen Peter A. Kind, Director US Army DISC4, 24 September 1993, UNCLASSIFIED.

[Kirk 1990] "Time Critical Communication Architecture: A Current Work Item Within Industrial Automation Systems (TC184) of ISO," M. Kirk, ERA Technology Limited, UK, *Military OSI Symposium Proceedings*, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[Klein 1993] *Guidance on Implementation of Reforms of Main Group Structure and Working Practices*, Memorandum to the Chairman, Vice-Chairman, and Principal Representatives to the TSGCE, DS(CC-ICP)(93)336, L. Klein, Head, Interoperability and Cooperative Programmes Section, International Military Staff, 26 May 1993, NATO UNCLASSIFIED.

[Knutsen 1993] "A Narrow-Band Tactical Message System with Packet-Radio Messaging and Interoperability with CCITT X.400," Kjell G. Knutsen, Alcatel Telecom AS (Norway), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Konoike 1987] "The Architecture of an Interoperable Database System Based on the OSI/RDA," Mitsuo Konoike, et al., Technical Committee 1, INTAP, *International Symposium on Interoperable Information Systems*, 25-27 February 1987.

[Kornfeld 1990] "Strengthening the US Standards Voice," Marilyn Kornfeld, *Computer Standards and Interfaces*, Volume 11, Number 2, 1990, p. 134.

[Krick 1991] *Submission of STANAG 4406 (Military Message Handling Systems) for Approval and Ratification*, DS(CCC-ICP)(91)710, Chairman WG2 (M. Krick), 10 December 1991, NATO UNCLASSIFIED.

[Krick 1991a] *MMHS AHWG Chairman's Report to WG2*, Review Draft, 30 September 1991, NATO UNCLASSIFIED.

[Kuhn 1990] *Briefing on X Window System Standards Update*, D. Richard Kuhn, Applications Portability Profile and Open Systems Environment Users Forum, US National Institute of Standards and Technology (NIST), Gaithersburg, MD, 9 May 1990.

[Kuhn 1991] *The X Window System Standards Update*, Richard Kuhn, NIST, 8th APP/OSE Workshop, NIST, Gaithersburg, MD, 12 November 1991.

[Lambert 1987] *X/OPEN On-Line Transaction Processing Reference Model*, Discussion Paper, M. G. Lambert, ICL, United Kingdom, July 1987.

[Lambert 1994] Private Communication with David W. Lambert, BICES Team, 27 January 1994.

[Landberg 1991] "OSE Implementor's Workshop," Ted Landberg, *8th APP/OSE Workshop*, NIST, Gaithersburg, MD, 12 November 1991.

[Lang 1989] *SIMNET Database Interchange Specification*, P. Wever, E. Lang, and C. S. Smyth, BBN Systems and Technologies Corporation and Spatial Data Research, Inc., BBN/DARPA Report 7108, July 1989.

[Lang 1990] "A Universal Data Exchange System," Pete Wever and Eric Lang, BBN Systems and Technologies Corporation, and C. Stephen Smyth, Spatial Data Research, Inc., *Geo'89 Symposium on Geographical Information Systems for Command and Control,* 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[Langeveld 1993] "Tactical Network to ISDN Interface Using STANAG 4206," Roger J. G. M. Langeveld, TNO Physics and Electronics Laboratory (The Netherlands), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993,* STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Langsford 1989] *Open Distributed Management Standards—The OSI Management Approach,* A. Langsford, Working Paper, July 1989.

[Law 1994] Private Communication from Steven Law on Operating System Services Standards, DISA/JIEO, 22 February 1994, UNCLASSIFIED.

[Lawn 1994] Private Communication on ACP 123 from Brian Lawn, SHAPE/CIS Division, 24 January 1994, NATO UNCLASSIFIED.

[LeGall 1991] "MPEG: A Video Compression Standard for Multimedia Applications," Didier LeGall, *Communications of the ACM,* Volume 34, Number 4, April 1991, pp. 47-58.

[Levine 1994a] Private Communication from Stan Levine on US Army ATCCS Architecture, OPM CHS, US Army CECOM, 18 January 1994.

[Levine 1994b] Private Communication from Stan Levine on US Army Common Hardware and Software, OPM CHS, US Army CECOM, 17 February 1994.

[Levine 1994c] Private Communication from Stan Levine on Protocols in the US Army Common Hardware and Software, OPM CHS, US Army CECOM, 18 February 1994.

[Liddell 1994] Private Communication from LTC Douglas Liddell, Army CIS Agency, UK MOD, Blandford Camp, 17 February 1994.

[Liou 1991] "Overview of the px64 Kbit/s Video Coding Standard," Ming L. Liou, *Communications of the ACM,* Volume 34, Number 4, April 1991, pp. 60-63.

[LLC 1988] *Optional LLC Security Sublayer,* Draft Proposed Addendum to IEEE 802.2 Logical Link Control, P802.2-88/95, Third Draft, IEEE, November 1988.

[Lynch 1991] "The Transition from TCP/IP to OSI," D. C. Lynch, *Journal of Information Systems,* Fall 1991.

[Macdonald 1993] "A Pragmatic Approach to Formal Methods and Protocols," Ruaridh Macdonald, Defence Research Agency-Malvern (United Kingdom), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993,* STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Maes 1991] *MIDS Programmers/Implementation Plans and Interoperability Requirements—NACMA Report of Activities,* NACMA(91), Guy Maes, NACMA/PID, 5 November 1991, NATO UNCLASSIFIED.

[Maggelet 1994] Private Communication with Joseph Maggelet, UNIX Systems Laboratory, 15 February 1993.

[Man 1990] *Telecommunication Management Network,* Working Document Prepared for the TSGCE SG9 AHWG on OSI Management, Man 0290/06, February 1990, NATO UNCLASSIFIED.

[Manno 1989] Private Communication with Salvatore J. Manno, Assistant Director for International Affairs, JTC3A, 24 October 1989, UNCLASSIFIED.

[Manno 1991] Private Communication with Salvatore J. Manno (US Representative to PG6), JTC3A, 9 December 1991, UNCLASSIFIED.

[Manno 1991a] *Report of the Tri-Service Group on Communications and Electronics (TSGCE), Subgroup on Communications, AC/302(SG/11) Meeting on 13-14 November 1991,* US Representative to SG11 (Salvatore J. Manno), 29 November 1991, NATO UNCLASSIFIED.

[Manno 1994] Private Communication with Salvatore J. Manno, DISA/JIEO, 4 January 1994, UNCLASSIFIED.

[Manvos 1989] *The X.400 Blue Book Comparison,* Carl-Uno Manvos, Technology Appraisals, London, 1989.

[Mapstone 1994] Private Communication on Standards Survey Review (through Gloria Furr-Fornshill), LTC Terry Mapstone, DISA/JIEO/TBC, 27 January 1994.

[Moraisin 1993] "RA90—The Future Bearer Service Network of the French Air Force," Christian Moraisin, Thomson-CFS (France), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Marine 1987] *Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP)*, Volume V, *Protocol Standard*, Headquarters, US Marine Corps, July 1987.

[Martin 1989] *Briefing on the Applications Portability Profile*, Roger J. Martin, US National Institute of Standards and Technology, 16 May 1989.

[Martin 1990] *Briefing on POSIX and Applications Portability*, Roger J. Martin, Institute for Computer Sciences and Technology, US National Institute of Standards and Technology, March 1990.

[Martin 1991] "NIST Update," Roger Martin, *13th JTAP Meeting*, CBEMA, 8 April 1991.

[Martin 1991a] "Applications Portability and Open Systems Environments: Status Report," Roger J. Martin, *APP/OSE Users' Forum*, NIST, 9 May 1991.

[Martin 1992] *A Federation of Software Engineering Environment Laboratories*, Roger J. Martin, National Institute of Science and Technology, 9 November 1992.

[Martin 1992a] "Open Systems Environments: IEEE OSE/POSIX Standards Status Report," Roger J. Martin, *NIST OSE/APP Forum*, 10 November 1992.

[Matthews 1990] "The Demand for Digital Geographic Products," Brigadier A. E. Matthews, Military Survey, UK MOD, *Geo'89 Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[McArthur 1991] *Analysis of X.400 Overhead*, L. McArthur and Lt K. Bryant (USN), JTC3A, 20 April 1991, UNCLASSIFIED.

[McCartney 1987] "Xcellence in Windows: Advantages of a Standard," I. McCartney, *Mini-Micro Systems*, Volume 20, Number 7, July 1987.

[McDermott 1991] *The Spatial Data Transfer Standard*, Matthew H. McDermott, *US Geological Survey*, 510 National Center, Reston, VA 22092 [paper to be presented at the American Congress of Surveying and Mapping's 1991 Annual Convention].

[McKellar 1990] "An Architecture for the Exchange of Geographic Data," David G. McKellar, Directorate of Cartography, National Defence Headquarters, Ottawa, Canada, *Geo'89 Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[McLane 1992] *US DoD Standards Process*, Richard S. McLane, 2 December 1992.

[McLane 1992a] *US SG9 Coordination Meeting Held 28 October 1992*, Richard McLane, US Representative, November 1992, UNCLASSIFIED.

[McLane 1992b] *Report of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution [AC/302(SG/9)] Meeting Held 2-4 December 1993*, Richard McLane, US Representative, December 1992, UNCLASSIFIED.

[McLane 1993a] *Report of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution [AC/302(SG/9)] Meeting Held 5-8 May 1993*, Richard McLane, US Representative, 8 May 1993, UNCLASSIFIED.

[McLane 1993b] *US SG9 Coordination Meeting Held 28 September 1993*, Richard McLane, US Representative, October 1993, UNCLASSIFIED.

[MDLA 1990] *Media Independent Data Link Architecture*, ADSIA-RCA-C-106-90, 28 May 1990, NATO UNCLASSIFIED.

[Mehta 1990] "User Interfaces and the IEEE P1201 Committee (Standards Report)," Sunil Mehta, *UNIX Review*, Volume 8, Issue 1 pp. 14-17, January 1990.

[Messeh 1991] *ISO/CCITT Collaborative Meeting on the Directory in Berlin from 21 October to 1 November 1991*, Letter to MAJ William Campbell, DISA/DEC, from Adel Messeh, National Telecommunications and Data Systems, 12 November 1991.

[Messina 1993] Private Communication with Larry Messina on DTMP Activities, December 1993.

[Messina 1993a] *Report of the Meeting of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution, Working Group 4 on Networking, AC302(SG/9)WG/5, Meeting 11-15 January 1993*, Larry Messina, US Representative, 10 February 1993, UNCLASSIFIED.

[Messina 1993b] *Report of the Meeting of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution, Working Group 4 on Networking, AC302(SG/9)WG/5, Meeting 19-23 April 1993,* Larry Messina, US Representative, April 1993, UNCLASSIFIED.

[Messina 1993c] *Report of the Meeting of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution, Working Group 4 on Networking, AC302(SG/9)WG/5, Meeting 5-July 1993,* Larry Messina, US Representative, 9 August 1993, UNCLASSIFIED.

[Messina 1993d] *Report of the Meeting of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution, Working Group 4 on Networking, AC302(SG/9)WG/5, Meeting 4-7 October 1993,* Larry Messina, US Representative, October 1993, UNCLASSIFIED.

[Messing 1990] *Performance of a Tactical Application Prototype Using GOSIP, Version 1,* Judy Messing, Shari Galitzer, and Calvin Lin, The MITRE Corporation, MTR-90W00209, December 1990.

[MIIDS IDB 1987] *Military Intelligence Integrated Data System (MIIDS) Integrated Data Bases (IDB) Definition and Specification Document (US),* DVP-2600-4537-87, Part I (NATO UNCLASSIFIED) and Part 2, *Data Element Catalog* (NATO CONFIDENTIAL), October 1987.

[Mills 1991] *Defense Standardized Profiles (DSPs),* Letter from NIST (Kevin Mills, Computer Systems Laboratory), to the DTMP, 30 July 1991.

[MITRE 1988] *The Department of Defense Open Systems Interconnection (OSI) Implementation Strategy,* The MITRE Corporation for the Defense Communications Engineering Center, May 1988.

[MITRE 1990] *Comments on the Applicability of Asynchronous Transfer Mode (ATM) to the Tactical Environment in the Year 2000 and Beyond,* MITRE, August 1990, UNCLASSIFIED.

[MITRE 1991] *DMS OSI Transition Plan,* Draft, Prepared for DISA by MITRE, 30 April 1991, UNCLASSIFIED.

[MITRE 1993] *Thin Stacks for Military Tactical Radio Applications,* Prepared by MITRE Washington C3I Networking Technical Center, September 1993, UNCLASSIFIED.

[MMHS 1990] *Intercept Profile for the Military Message Handling System (MMHS), Issue 2,* March 1990, NATO UNCLASSIFIED.

[MOD 1989] *Scope for MOD Information Technology (IT) Standardization and Responsibilities,* UK MOD Information Technology Standards Board, 11 August 1989.

[MODITSB 1989] *Scope for MOD IT Standardization and Responsibilities, MOD Information Technology Standards Board Executive Committee Technical Group,* MODITSB 3/89, 11 August 1989.

[Montgomery 1989] *GEMINI: Government Expert Systems Methodology Initiative,* T. A. Montgomery and E. Crispin, Fifth International Expert Systems Conference, London, 6-8 June 1989, pp. 45-54.

[Moulton 1992] *Multicast Transport Service Definition,* J. Moulton, X3S3.3-92-201, May 1992.

[MPMC 1991] *Open Systems Interconnect (OSI) Multipeer/Multicast (MPMC) Prospectus,* Center for Communications and Signal Processing and Communications-Electronics Command, 4 November 1991, p. 8.

[MROC 3-88 1989] *Implementation of Multicommand Required Operational Capability (MROC) 3-88, The Defense Mapping System (DMS),* Director for C3 Systems, Joint Staff, 6 February 1989, UNCLASSIFIED.

[MTS TIDP 1987] *Technical Interface Design Plan for Marine Tactical Systems (MTS TIDP),* Volume V, Protocol Standard, Headquarters, US Marine Corps, July 1987, UNCLASSIFIED.

[NACISA 1988] *Standard Automated Message Interface for NATO ACCIS (STAMINA), Version 3.0 with Amendment List 1,* NACISA/ISD/CCISPT(88)394E, NACISA, 17 November 1988, NATO UNCLASSIFIED.

[NACISA 1989] *NATO C3 Architecture (U),* Volume 1, *Consolidated Architecture (U),* NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989a] *NATO C3 Architecture (U),* Volume 2, *Headquarters and Facilities Subsystem (U),* NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989b] *NATO C3 Architecture (U),* Volume 3, *Information System Subsystem (U),* NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989c] *NATO C3 Architecture (U),* Volume 4, *Communications Subsystem (U),* NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1989d] *NATO C3 Architecture (U),* Volume 5, *Sensor and Warning Installations Subsystem (U),* NACISA/APD/C3AB(89)101, NACISA, 31 May 1989, NATO CONFIDENTIAL.

[NACISA 1990] *Statement to TSGCE SG/9 on STAMINA and Related Activities*, NACISA, May 1990, NATO UNCLASSIFIED.

[NACISA 1992] *NATO C3 Physical Communications Architecture–Recommended Topology*, NACISA/APD/C3AB(92)50, May 1992, NATO UNCLASSIFIED.

[NACISA 1993a] *Introduction of New Message Handling Procedures*, NACISA/APD/C3AB(92)006, Director General NACISA, 16 January 1992, NATO UNCLASSIFIED.

[NACISC 1988] *NATO Bodies in the Fields of Communications and Information Systems*, AC/317-D/23, NACISC, April 1988, NATO UNCLASSIFIED.

[NACISC 1989] *NATO Consultation, Command and Control (C3) Master Plan (U)*, Edition 1, AC/317-WP-66 (J-1800/77/5), Information Systems Working Group (ISWG) and Communications Systems Working Group (CSWG) of the NATO Communications and Information Systems Committee (NACISC), July 1989, NATO CONFIDENTIAL.

[NACISC 1989a] *TRI-Major NATO Commanders' Command and Control (C2) Plan (U), 2300.12.5/SHORC/89, Edition 4*, ISWG and CSWG of the NACISC, 20 July 1989, NATO SECRET.

[NACISC 1989b] *Political Consultation and NATO Civil Emergency Planning (PCNCEP) CIS Plan (U)*, Edition 1, AC/317(WG/1)WP/36 (Revised) and AC/317(WG/2)WP/51 (Revised) (J-1800/77/6), ISWG and CSWG of the NACISC, 18 July 1989, NATO CONFIDENTIAL.

[NACISC 1989c] *Working Relationships*, Note by the Secretary, AC/317-N/185, NACISC, 24 February 1989, NATO UNCLASSIFIED.

[NACISC 1990] *Data Management*, AC/317(WG/2)WP/60, NACISC, 5 June 1990.

[NACISC 1992a] *NATO ISO Naming and Addressing Authority*, AC/317-N/399, M. Baptista Coelho, NACISC, 30 January 1992, NATO UNCLASSIFIED.

[NACISC 1992b] *Integrated ACCS/CIS Communication Architecture*, AC/317-N/419 [NACMO(BOD)N/55], 1992, NATO RESTRICTED.

[NACISC 1993a] *NATO Data Management Policy*, AC/317-D/61, NACISC (Note by the Military Secretary), 29 June 1993, NATO UNCLASSIFIED (approved by the CSWG/ISWG .

[NACISC 1993b] *1992 Annual Report by the Chairman of the Allied Data Systems Interoperability Agency (ADSIA)*, AC/317-N/504 (Note by the Military Secretary), NACISC, 25 February 1993, NATO UNCLASSIFIED.

[NACISC 1993c] *NATO Management Information System (MIS) Policy*, Working Paper, AC/317(WG/2)WP/84, 6 August 1993, NATO UNCLASSIFIED.

[NACISC 1993d] *Software Methods and Tools Study*, Working Paper, AC/317(WG/2)WP/83, ISWG, NACISC, 22 July 1993, NATO UNCLASSIFIED.

[NACISC 1993e] *NATO Software Standards*, Document, AC/317-D/59, 22 March 1993, NATO UNCLASSIFIED.

[NACISC 1993f] *Future Activities of the NATO CIS Community*, Working Paper, AC/317-WP/190(Revised), 3 December 1993, NATO UNCLASSIFIED.

[NACISC 1993g] *Future Activities of the NATO CIS Community—Work Plan*, Working Paper, Addendum to AC/317-WP/190(Revised), 22 December 1993, NATO UNCLASSIFIED.

[NACISC 1993h] *General Guidance on the Security of ADP Systems and Networks*, Working Paper, AC/317(WG/2)WP/88, ISWG, NACISC, 29 November 1993, NATO UNCLASSIFIED.

[NACISC 1993i] *ISWG Work Plan*, Note, AC/317(WG/2)N/384, ISWG, NACISC, 1 March 1993, NATO UNCLASSIFIED.

[NACMA 1992] *The Air Command and Control System Programme*, Briefing, OGM/sc-10/92, Office of the General Manager, NATO Air Command and Control System Management Agency (NACMA), 13 October 1992, NATO UNCLASSIFIED.

[NACMA 1993a] *Portability Discussion Paper*, NACMA(93)871, Iga A. Laget, Deputy General Manager, NATO Air Command and Control System Management Agency (NACMA), 4 June 1993, NATO UNCLASSIFIED.

[NACMA 1993b] *Air Command and Control System (ACCS) Reference Brochure*, NATO Air Command and Control System Management Agency (NACMA), 1993, NATO UNCLASSIFIED.

[NACMA 1993c] *The NATO Air Command and Control System Programme*, NACMA, 13 October 1993, NATO UNCLASSIFIED.

[NAPI 1992] "Formation of a North American PCTE Initiative (NAPI)," *NIST ISEE Users' Forum*, 9 November 1992.

[NATO 1987] *Issues Within the NATO Military Data Communications Internetwork*, Draft Working Paper, TSGCE SG9, 1 September 1987, NATO UNCLASSIFIED.

[NATO 1987a] *NATO Naval Intra-Ship Tactical Control and Data Handling Open Systems Interconnection, Network Independent Interface, Transport Service Definition for Connection-Mode Transmission*, Proposed Draft STANAG, 16 September 1987, NATO UNCLASSIFIED.

[NATO 1989a] *NATO Network Security Information Classification Guide (NU)*, Version 1.0, TSGCE SG9, February 1989, NATO RESTRICTED.

[NATO 1989b] *The North Atlantic Treaty Organization—Facts and Figures*, NATO, 1989.

[NATO 1990] *Proceedings of the Military OSI Symposium*, Volume 3, June 1990, NATO SECRET.

[NATO 1990a] *UK MOD Contribution to TSGCE SG9/WG1*, 23 July 1990, NATO UNCLASSIFIED.

[NATO 1991] *NATO Technical Interface Standards (NTIS) Transition Strategy, Sixth Edition*, AC/259-D/1218(Revised), *Conference of National Armaments Directors* (CNAD), *Tri-Service Group on Communications and Electronic Equipment* (TSGCE), NATO, Brussels, 11 November 1991, NATO UNCLASSIFIED.

[NATO 1993a] *NATO Open Systems Interconnection Profile (NOSIP) Strategy*, Draft, Working Paper AC/302(SG/9)WP/32 , TSGCE Subgroup 9, 20 September 1993, NATO UNCLASSIFIED.

[NATO 1993b] *NATO Open Systems Environment Baseline Architectural Principles*, Appendix 1 to Annex to AC/317(WG2)WP/82, Final Draft, NACISC/ISWG, 22 June 1993, NATO UNCLASSIFIED.

[NATO 1993c] *NATO Open Systems Environment Reference Model*, Appendix 2 to Annex to AC/317(WG2)WP/82, Final Draft, NACISC/ISWG, 22 June 1993, NATO UNCLASSIFIED.

[NATO 1993d] *NATO Open Systems Environment Base Standards*, Draft, Ada Implementation Subgroup, NACISC/ISWG, 23 August 1993, NATO UNCLASSIFIED.

[NATO HQ 1992] *Army Tactical Command and Control information System Working Paper 25, Technical Standards for CCISs*, DS(CCC-IP)(92)123, AC/302(SG9), ICP Section, C3 Directorate, NATO Headquarters International Staff, 25 February 1992, NATO UNCLASSIFIED.

[NATO MC 1987] *Memorandum ISM-UAK-7, NATO Military Committee*, 12 January 1987.

[NATO Naval 1987] *NATO Naval Intra-Ship Tactical Control and Data Handling Open Systems Interconnection, Network Independent Interface, Transport Service Definition for Connection-Mode Transmission*, Proposed Draft STANAG, 16 September 1987, NATO UNCLASSIFIED.

[NATO OSE 1993] *NATO Open Systems Environment (OSE)—Baseline Architectural Principles and Reference Model*, AC/317(WG/2)WP/82, NACISC/ISWG (Note by the Military Secretary), 19 July 1993, NATO UNCLASSIFIED: Volume I, *Baseline Architectural Principles* (Draft, 22 June 1993); Volume 2, *Reference Model* (Draft, 23 June 1993); and Volume 4, *Base Standards* (Draft Version 5.3, 23 November 1993).

[NGCR 1993b] *Reference Model for Support Environments*, Next Generation Computer Resources, Version 2.0, 2 September 1993.

[Neve 1990] Private Communication with Nick Neve, RSRE, UK MOD, 22 March 1990.

[Nevergold 1993] "NATO C3 Communications Architecture Topology and Topography of the Circuit Switched Network," Richard U. Nevergold and Robert C. Sivills, USNATEX/NACISA (MITRE USDC3FOI) (Belgium), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Newcomb c1991] *The Hypermedia/Time-based Document Structuring Language "HyTime,"* Steven R. Newcomb, Neill A. Kipp, and Victoria T. Newcomb, n.d.

[NIAG 1989] *Programme of Work 1990-1992, Issue 1*, NIAG SG/6 on the Compatibility of Naval Data Handling Equipment, December 1989, NATO UNCLASSIFIED.

[Nicholas 1992] *On the Interchangeability of SGML and ODA*, Charles K. Nicholas and Lawrence A. Welsch, National Institute of Standards and Technology, NISTIR 4681, January 1992.

[Nieporent 1990] *Use of OSI Protocols for US Army Tactical Command and Control Applications*, Richard Nieporent and Brajesh Mishra, The MITRE Corporation, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[NIIF 1989] *Briefing on NACISA Interface Initiative (NIIF) to TSGCE SG/9 WG/1*, June 1989, NATO UNCLASSIFIED.

[NIMP 1988] *NATO Interoperability Management Plan (NIMP)*, CNAD/NACISC, AC/259-D/1274 and AC/317-D/33, Second Edition, 1988, NATO UNCLASSIFIED.

[NIPD 1993] *NATO Interoperability Planning Document*, Allied Data Systems Interoperability Agency, 1 January 1993, NATO UNCLASSIFIED: Volume I, *Organization of NATO Information*

Systems Interoperability; Volume II, *Formal Specification of Information Exchange Requirements;* Volume III, *Plan for the Development of NATO Common Interoperability Standards;* Volume IV, *Plan for the Configuration Management of NATO Common Interoperability Standards;* Volume V, *Testing Concept for NATO Common Interoperability Standards;* Volume VI, *Documentation Plan for NATO Common Interoperability Standards.*

[NIST 1987] *Guide on Data Entity Naming Conventions,* NIST SP 500-149, US National Institute of Standards and Technology, October 1987.

[NIST 1988] *Stable Implementation Agreements for Open Systems Interconnection Protocols,* Version 2, Edition 1, NIST Special Publication 500-16, US National Institute of Standards and Technology, December 1988.

[NIST 1989] *Ongoing Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements,* NISTIR 88-3824-2, National Institute of Standards and Technology, February 1989.

[NIST 1990] *Open Systems Standards: A Federal Strategy,* US National Institute for Standards and Technology, Undated (Provide to IDA on 30 April 1990).

[NIST 1990a] *Briefing on POSIX,* US National Institute of Standards and Technology, 12 June 1990.

[NIST 1990b] *Stable Implementation Agreements for Open Systems Interconnection Protocols,* Version 3, Edition 1, NIST Special Publication 500-177, National Institute of Standards and Technology, March 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop; basis for US GOSIP 2.0).

[NIST 1990c] *Working Agreements. Working Implementation Agreements for Open Systems Interconnection Protocols: Continuing Agreements,* Volume 2, Number 2, NISTIR 90-4247, National Institute of Standards and Technology, February 1990 (Proceedings of December 1989 NIST OSI Implementor's Workshop).

[NIST 1991] *Stable Implementation Agreements for Open Systems Interconnection Protocols,* Version 5, Edition 1, National Institute of Standards and Technology, NIST Special Publication, SP 500-202, December 1991.

[NIST 1993] *APP: Application Portability Profile: The US Government's Open System Environment Profile OSE/1,* Version 2.0, NIST Special Publication 500-210, NIST, June 1993.

[NIST 1993a] *Stable Implementation Agreements for Open Systems Interconnection Protocols,* NIST, December 1993.

[NMICC 1989] *NATO Maritime Interface Coordination Center Support and Capability* (NMICC) *Project Data and Justification* (U), NATO Common Funded Infrastructure, Third Revision, January 1989, NATO CONFIDENTIAL.

[Nolan 1990] *CASE Integration Services: Technical Description,* Chris J. Nolan, CIS 90-008, 31 March 1990.

[NOSA 1988] *NATO OSI Security Architecture* (NOSA), Ad Hoc Working Group on Security, TSGCE SG9, Draft Version 2.1, March 1988, NATO UNCLASSIFIED.

[NSA 1989] *Secure Data Network System* (SDNS) *Security Protocol 3* (SP3), Specification SDN.301, Revision 1.5, SDNS *Protocol and Signalling Working Group,* 15 May 1989, National Security Agency.

[NSA 1989a] *Secure Data Network System* (SDNS) Security Protocol 4 (SP4), Specification SDN.401, Revision 1.3, SDNS *Protocol and Signalling Working Group,* 2 May 1989, National Security Agency.

[NSA 1989b] *Secure Data Network System* (SDNS) *Key Management Profile, Communication Protocol Requirements for Support of the SDNS Key Management Protocol,* Specification SDN.601, Revision 1.5, SDNS Protocol and Signalling Working Group, 11 August 1989, National Security Agency.

[NSA 1989c] *Secure Data Network System* (SDNS) Message Security Protocol (MSP), Specification SDN.701, Revision 1.5, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989d] *Secure Data Network System* (SDNS) *Directory Specifications for Utilization with the SDNS Message Security Protocol* (MSP), Specification SDN.702, Revision 1.4, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989e] *Secure Data Network System* (SDNS) *Access Control Concept Document,* Specification SDN.801, Revision 1.3, SDNS Protocol and Signalling Working Group, 26 July 1989, National Security Agency.

[NSA 1989f] *Secure Data Network System* (SDNS) Access Control Specification, Specification SDN.802, Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency.

[NSA 1989g] *Secure Data Network System* (SDNS) *Access Control Specification, Addendum 1, Access Control Information Specification* (ACIS), Specification SDN.802/1, Revision 1.0, SDNS Protocol and Signalling Working Group, 25 July 1989, National Security Agency.

[NSA 1989h] *Secure Data Network System* (SDNS) *Key Management Protocol, Definition of Services Provided by the Key Management Application Service Element* (KMASE), Specification SDN.902, Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989i] *Secure Data Network System* (SDNS) *Key Management Protocol, Specification of the Protocol for Services Provided by the Key Management Application Service Element* (KMASE), Specification SDN.903, Revision 3.2, SDNS Protocol and Signalling Working Group, 1 August 1989, National Security Agency.

[NSA 1989j] *Secure Data Network System (SDNS) Key Management Protocol, SDNS Traffic Key Attribute Negotiation*, Specification SDN.906, Revision 1.3b, SDNS Protocol and Signalling Working Group, 18 September 1989, National Security Agency.

[NST 1988] *NATO Staff Target (NST) for the Battlefield Information Collection and Exploitation Systems (U)*, AC/302-D/560, AC/302(PG/7)D/20 (Revised), 28 December 1988, NATO CONFIDENTIAL.

[Oberndorf 1992] *Next Generation Computer Resources (NGCR) - Project Support Environment Standards Working Group (PSESWG) Program and Environment Reference Model*, Patricia Oberndorf, Naval Air Warfare Center, 9 November 1992.

[Oldenburg 1989] "OSF Motif, the User Interface Standard," H. Oldenburg, IEEE Colloquium on User Interface Management Systems, *Digest*, Number 135, Issue 2, IEEE, 17 November 1989.

[OMNICON 1987] *The OMNICON Index of Standards for Distributed Information and Telecommunication Systems*, OMNICON, 1987.

[Onufer 1990] *Functional Profiles for Open Systems Interconnection*, Joseph R. Onufer, TSGCE SG9 WG1, US Army CECOM ISD, Military OSI Symposium, Symposium Proceedings SP-8, Volume 1, 5-8 June 1990.

[Onufer 1991] *Report of the US Representative (Joe Onufer) of the Ad Hoc Meeting on the NATO Open Systems Interoperability Plan (NOSIP), 25 to 27 September 1991*, 16 October 1991, UNCLASSIFIED.

[Onufer 1991a] *Report to SG9 by the Chairman of WG1 on Layers 1-4*, Joe Onufer, 10 December 1991, NATO UNCLASSIFIED.

[Onufer 1991b] *WG/1 Statement on the Future of Layer STANAGs and Future Terms of Reference*, TSGCE SG9/WG1, October 1991, NATO UNCLASSIFIED.

[Onufer 1991c] *Response to WG1 AI910521 Relating to the WG1 TOR and 18-Month Work Plan*, Chairman (Joe Onufer) WG1, 27 June 1991, NATO UNCLASSIFIED.

[Onufer 1991d] *Chairman's Report of the May 1991 WG1 Meeting*, Chairman (Joe Onufer) WG1, 26 August 1991, NATO UNCLASSIFIED.

[Onufer 1992a] *Report of the Meeting of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution, Working Group 4 on Networking, AC302(SG/9)WG/5, Ad Hoc Working Group on Functional Profiles, Held 6-10 July 1992*, Joe Onufer, Chairman, 27 September 1992 (Revised 8 December 1992), UNCLASSIFIED.

[Onufer 1992b] *Report of the Meeting of the Tri-Service Group on Communications and Electronics (TSGCE) Subgroup 9 on Data Distribution, Working Group 4 on Networking, AC302(SG/9)WG/5, Meeting 5-9 October 1993*, Joe Onufer, Chairman, 1 December 1992 (Revised 17 December 1992), UNCLASSIFIED.

[Onufer 1993] *Future Programme of Work*, AC/302(SG/9)WG/5-931035, Joe Onufer, Chairman, October 1993, NATO UNCLASSIFIED.

[OP-094 1991] *Fleet Communications in the Copernicus Architecture*, Final Draft, June 1991, UNCLASSIFIED; *The Copernicus Architecture*, Briefing to IDA, Space and Electronic Warfare Directorate OP-094 (CAPT J. R. Wood), October 1991, UNCLASSIFIED.

[ORACLE 1994] *Trusted ORACLE7 Technical Overview*, ORACLE Corporation, January 1994, UNCLASSIFIED.

[Ornstein 1991] Private Communication with David Ornstein, 4 April 1991.

[OSE 1993] *Guide on Open System Environment (OSE) Procurements,* Gary E. Fisher, Systems and Software Technology Division, Computer Systems Laboratory, NIST, Draft, 12 November 1993.

[OSF 1990] *Announcement of Technology Selection,* Distributed Computing Environment Request for Technology (RFT), Open Software Foundation, 14 May 1990.

[OSF 1990a] *OSF/Motif: The Graphical User Interface for Open Systems, A White Paper,* OSF, October 1990.

[OSN 1988] "X.400 1988 and X.500 (The Directory) Make Their Debut," *OSN: The Open Systems Newsletter,* Volume 2, Issue 8, Technology Appraisals, Limited, London, October 1988.

[OSN 1988a] "Open Systems Opening Up," *OSN: The Open Systems Newsletter,* Volume 2, Issue 9/10, Technology Appraisals, Limited, London, November/ December 1988.

[OSN 1988b] "EDI1—CCITT Takes First Steps to X.400 and EDI Convergence," *OSN: The Open Systems Newsletter,* Volume 2, Issue 7, Technology Appraisals, Limited, London, September 1988.

[OSN 1989] "OSITOP Reports on Progress," *OSN: The Open Systems Newsletter,* Volume 3, Issue 3, Technology Appraisals, Limited, London, March 1989.

[OSN 1989a] "Harmonization Between Document Filing and Retrieval (DFR) and FTAM," *OSN: The Open Systems Newsletter,* Volume 3, Issue 12, December 1989.

[OSN 1989b] "The ISO Virtual Terminal Standards," *OSN: The Open Systems Newsletter,* Volume 3, Issue 4, Technology Appraisals, Limited, April 1989.

[OSN 1989c] *OSN: The Open Systems Newsletter,* Volume 3, Issue 1, January 1989.

[OSN 1990] "OSF Releases OSF/1 Version 1.0," *OSN: The Open Systems Newsletter,* Volume 4, Issue 12, December 1990, p. 18.

[OSN 1990a] *OSN: The Open Systems Newsletter,* Volume 4 Issue 1/Issue 2, January/February 1990, pp. 17-18.

[OSN 1990b] "Towards Routing Standards for OSI Networks" *OSN: The Open Systems Newsletter,* December 1990, Volume 4, Issue 12, p. 10.

[OSN 1990c] "What is Next in Distributed Computing?" *OSN: The Open Systems Newsletter,* December 1990, Volume 4, Issue 12, p. 3.

[OSN 1990d] *OSN: The Open Systems Newsletter,* Volume 4, Issue 3, March 1990, pp. 14-18.

[OSN 1990e] *OSN: The Open Systems Newsletter,* Volume 4, Issue 3, March 1990, pp. 9-11.

[OSN 1990f] *OSN: The Open Systems Newsletter,* Volume 4, Issue 4, April 1990, p. 4.

[OSN 1990g] "What is Next in Distributed Computing?" *OSN: The Open Systems Newsletter,* December 1990, Volume 4, Issue 12, pp. 1-5.

[OSN 1990h] *OSN: The Open Systems Newsletter,* Volume 4, Issue 4, April 1990, p. 10.

[OSN 1990j] *OSN: The Open Systems Newsletter,* Volume 4, Issue 3, March 1990, pp. 24-25.

[OSN 1991] "OSF Announces Qualifying Submitters in DME RFT," *OSN: The Open Systems Newsletter,* Market Messages, Volume 5, Issue, 1, January 1991, pp. 20-21.

[OSN 1991a] "NTT Announces Standards for Multivendor Computer Systems," *OSN: The Open Systems Newsletter,* Volume 5, Issue 1, January 1991, p. 20.

[OSN 1991b] "Open Document Architecture: The Emerging Market," *OSN: The Open Systems Newsletter,* Volume 5, Issue 3, March 1991, pp. 19-23.

[OSN 1991c] "EWOS Reports on Progress, " *OSN: The Open Systems Newsletter,* Volume 5, Issue 3, March 1991, pp. 7-10.

[OSN 1991d] "Open Document Architecture Standard Comes of Age," *OSN: The Open Systems Newsletter,* Volume 5, Issue 4, April 1991, pp. 4-8.

[OSN 1991e] "What is New in US GOSIP - Profile of a Profile," *OSN: The Open Systems Newsletter,* Volume 5, Issue 1, January 1991, p. 4.

[OSN 1991g] "EPHOS: Phase I Agreed as Phase II Begins," *OSN: The Open Systems Newsletter,* Volume 5, Issue 4, April 1991, pp. 1-3.

[OSN 1991h] "OSINET Joints COS," *OSN: The Open Systems Newsletter,* Volume 5, Issue 1, January 1991, p. 23.

[OSN 1991i] "GOSIP 4 - The New Version of UK GOSIP now Available," *OSN: The Open Systems Newsletter,* Volume 5, Issue 7, July 1991, pp. 19-20.

[OSN 1991j] "Understanding Open Distributed Processing," *OSN: The Open Systems Newsletter,* Volume 5, Issue 9, September 1991, pp. 1-18.

[OSN 1991k] "Latest SC18 Work Programme," *OSN: The Open Systems Newsletter*, Volume 5, Issue 9, September 1991, p. 26.

[OSN 1991m] "GOSIP 4 - The New Version of UK GOSIP Now Available," *OSN: The Open Systems Newsletter*, Volume 5, Issue 7, July 1991, pp. 19-20.

[OSN 1991n] "COSINE on Target for 1992," *OSN: The Open Systems Newsletter*, Volume 5, Issue 5/6, May/June 1991, pp. 14-17.

[OSN 1992] "IBM's Networks—A Little More Open," *OSN: The Open Systems Newsletter*, April 1992, pp. 1-3.

[OSN 1992a] "X.400 and FTAM: Which is Best for You?" *OSN: The Open System Newsletter*, Volume 6, Number 5, May 1992, pp. 16-20.

[OSN 1992b] "X.500, An OSI Success Story", *OSN: The Open System Newsletter*, Volume 6, Number 4, April 1992, pp. 20-22.

[OSN 1992c] "OSF Plans for OSF/1 and MOTIF," *OSN: The Open Systems Newsletter*, Volume 6, Number 8, July/August 1992, pp. 5-9.

[OSN 1992d] "OSI NM: Cautious Users Demand Words, Not Deeds," *OSN: The Open Systems Newsletter*, Volume 6, Issue 4, April 1992, pp. 22-23.

[OSN 1992e] "A Roadmap for Open Management," *OSN: The Open Systems Newsletter*, Volume 6, Issue 5, May 1992, pp. 12-16.

[OSN 1992f] "Omnipoint Squares CMIP and SNMP?" *OSN: The Open Systems Newsletter*, Volume 6, Issue 9, September 1992, p. 28.

[OSN 1992g] "Standard for Cheap Window Terminals Nears the Market," *OSN: The Open Systems Newsletter*, Volume 6, Issue 2, February 1992, pp. 30-31.

[OSN 1992h] "X/Open's New Look Research and Branding Programmes," *OSN: The Open Systems Newsletter*, Volume 6, Issue 5, May 1992, pp. 20-21.

[OSN 1992i] "XPG4 Details: DCE is In," *OSN: The Open Systems Newsletter*, Volume 6, Issue 9, September 1992, p. 26.

[OSN 1992j] "Omnipoint: How to Manage CMIP and SNMP," *OSN: The Open Systems Newsletter*, Volume 6, Issue 10, October 1992, pp. 1-8.

[OSN 1992k] "A Renaissance for X/Open?," *OSN: The Open Systems Newsletter*, Volume 6, Issue 10, October 1992, pp. 9-12.

[OSN 1992l] "The Latest News on the X Window System," *OSN: The Open Systems Newsletter*, Volume 6, Issue 10, October 1992, pp. 12-17.

[OSN 1992m] "ISO Distributed Systems Work Progresses," *OSN: The Open Systems Newsletter*, Volume 6, Issue 10, October 1992, pp. 17-22.

[OSN 1992n] "Market Messages: ISO's Olive Branch to Internet," *OSN: The Open Systems Newsletter*, Volume 6, Issue 10, October 1992, p. 25.

[OSN 1992o] "ISODE Meets the Real World," *OSN: The Open Systems Newsletter*, Volume 6, Issue 12, December 1992, pp. 14-18.

[OSN 1993] "Open Forum - The Show Will Go On?," *OSN: The Open Systems Newsletter*, Volume 7, Issue 1, January 1993, pp. 11-16.

[OSN 1993a] "Market Messages: New X Body to Form," *OSN: The Open Systems Newsletter*, Volume 7, Issue 1, January 1993, pp. 19-20.

[OSN 1993b] "Implementing Forms-Mode VT," *OSN: The Open Systems Newsletter*, Volume 7, Issue 2, February 1993, pp. 10-17.

[OSN 1993c] "Where is DCE?," *OSN: The Open Systems Newsletter*, Volume 7, Issue 3, March 1993, pp. 1-9.

[OSN 1993d] "UI Moves Towards RFTs for Multimedia and Other UNIX Technology," *OSN: The Open Systems Newsletter*, Volume 7, Issue 3, March 1993, p. 22.

[OSN 1993e] "A Reference Model for Systems Builders?," *OSN: The Open Systems Newsletter*, Volume 7, Issue 4, April 1993, pp. 7-17.

[OSN 1993f] "COSE Kills Open Look, Promises UNIX Unity," *OSN: The Open Systems Newsletter*, Volume 7, Issue 4, April 1993, p. 18.

[OSN 1993g] "A de facto Standard for Desktop Management," *OSN: The Open Systems Newsletter*, Volume 7, Issue 6, June 1993, pp. 1-10.

[OSN 1993h] "Can you Rely on POSIX," *OSN: The Open Systems Newsletter*, Volume 7, Issue 6, June 1993, pp. 10-16.

[OSN 1993i] "UI Asks for Cut and Paste Technology," *OSN: The Open Systems Newsletter*, Volume 7, Issue 6, June 1993, pp. 24-25.

[OSN 1993j] "Fast Switch to C++," *OSN: The Open Systems Newsletter*, Volume 7, Issue 6, June 1993, p. 26.

[OSN 1993k] "Users Deserve Better Repositories," *OSN: The Open Systems Newsletter*, Volume 7, Issue 6, June 1993, p. 27.

[OSN 1993l] "Windows NT Support Spreads," *OSN: The Open Systems Newsletter*, Volume 7, Issue 6, June 1993, p. 28.

[OSN 1993m] "Microsoft's ODBC Gains Support," *OSN: The Open Systems Newsletter*, Volume 7, Issue 6, June 1993, p. 31.

[OSN 1993n] "COSE - A New Standards Process?," *OSN: The Open Systems Newsletter*, Volume 7, Issue 8, August 1993, pp. 1-7.

[OSN 1993o] "SPAG Under Notice," *OSN: The Open Systems Newsletter*, Volume 7, Issue 8, August 1993, pp. 24-25.

[OSN 1993p] "Multimedia Communications Group," *OSN: The Open Systems Newsletter*, Volume 7, Issue 8, August 1993, pp. 27-28.

[OSN 1993q] "X/Open Takes Charge of UNIX," *OSN: The Open Systems Newsletter*, Volume 7, Issue 9, September 1993, pp. 1-4.

[OSN 1993r] "X/Open Acquires UNIX Trademark," *OSN: The Open Systems Newsletter*, Volume 7, Issue 10, October 1993, pp. 1-7.

[OSN 1993s] "The End of API: A Win for IBM?," *OSN: The Open Systems Newsletter*, Volume 7, Issue 9, September 1993, p. 19.

[OSN 1993t] "TSPIRIT: Open Systems for Telcos," *OSN: The Open Systems Newsletter*, Volume 7, Issue 10, October 1993, pp. 7-11.

[OSS 1993] "Charting the Path to a National Information Infrastructure," *Open Systems Standards Tracking Report*, Volume 2, Number 5, October 1993, pp. 1-3. .

[P1003.0 Guide 1993] *Draft Guide to the POSIX Open System Environment*, Draft 16.1, IEEE, October 1993.

[P1175 1989] "Proposed Standard Eases Tool Interconnection," IEEE Software, November 1989, pp. 69-70.

[P1252 1991] "Standards Actions of the IEEE Standards Board, March 21, 1991," *The IEEE Standards Bearer*, Volume 5, Number 1, April 1991, p. 8.

[Pait 1994] Private Communication from MAJ Michel Pait on Standards—Past, Present, and Future, HQ USAF/SCTA, 16 February 1994, UNCLASSIFIED.

[Pant 1991] *Packet Multicast Service Definition (X.PMS)*, Draft Version 1.3, R. Pant, Associate Rapporteur on Q1 (Multicast), ANSI X3S3.7/91-73, 4 June 1991, UNCLASSIFIED.

[Payton 1988] "Standard Status—SC21 Information Retrieval, Transfer, and Management of OSI," Alan Payton, *OSN: The Open System Newsletter*, Volume 2, Issue 5, Technology Appraisals, Limited, London, July 1988.

[PC 1989] Private Communication with the Chair of the TSGCE SG9 Ad Hoc Working Group on Security, 21 March 1989.

[PCTE 1989] "PCTE as a Proposed ISO," *Computer Systems Europe*, January 1989.

[PDES, Inc.] *STEP Brochure*, PDES, Inc. 5300 International Boulevard, North Charleston, SC 29418, (803) 760-3342.

[PDTR 10167 1989] *Guidelines for the Application of Estelle*, LOTOS and SDL, PDTR 10167, ISO/IEC JTC1/SC21 (SC21 N 3252), February 1989.

[Pennington 1993] "Integrated Tactical-Strategic Data Networking," Catherine Pennington, MITRE (United States), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Perez 1991] Private Communication with Sandra Perez, Concept Technology, Inc., (703) 425-9268, 23 April 1991.

[Pilla 1991] *Report of the Tri-Service Group on Communications and Electronics (TSGCE), Subgroup on Communications, AC/302(SG/11) Meeting on 13-14 November 1991*, US Representative to SG11 (Lou Pilla), 29 November 1991, NATO UNCLASSIFIED.

[Pink 1991] *Conformance Testing from the European Point of View*, Jane Pink and Jon Leigh, National Centre for Information Technology, 7th OSE/APP Users' Forum, May 9, 1991, NIST, Gaithersburg, MD.

[PNL 1994] Private Communication from Pacific Northwest Laboratories on Fire Support Systems, January 1994, UNCLASSIFIED.

[Prast 1994] Private Communication from Gerald Prast, Royal Netherlands Army, Directorate of Economy and Finance, 18 February 1994.

[PRC 1988] *Army Implementation of DoD and Federal Standards*, Draft, Prepared for US Army Information Systems Engineering Command by Planning Research Corporation, 8 May 1988.

[Price 1990] *Practical Evaluation of OSI Protocols*, J. Price, D. B. Hearn, J. Laws, A. F. Martin, and J. Staromlynska, RSRE, UK MOD, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Price 1991] "Standard for Data Dictionaries Now Is Mandatory," Douglas S. Price, *Government Computer News*, Volume 10 Number 8, April 15, 1991, p. 60.

[PSC 1991] *X.400 Message Handling Systems: 1992 and Beyond*, Briefing, Protocol Standards and Communications, Inc., and Technology Appraisals, 1991.

[PSSG 1991] *Minutes of the Protocol Standards Steering Group (PSSG)*, 43rd Meeting - 8-9 January 1991.

[PSTP 1991] *Recommendations for DoD Actions to Assure GOSIP Message Handling Systems Suitability for Military Requirements, Protocol Standards Technical Panel (PSTP) Working Group Three (Message Handling Systems)*, Revised, 8 January 1991.

[Purton 1987] *Draft Compilation of OSI Standards*, M. J. Purton, Unpublished, August 1987.

[Putnam 1982] *The Impacts of Private Voluntary Standards on Industrial Innovation*, Putnam, Hayes, and Bartlett, Inc., Prepared for National Bureau of Standards, Washington, D.C., 1982.

[QIC 1988] *Quadrilateral Tactical Interface Requirement, Version 2*, Quadrilateral Interface Committee, 1 August 1988, UNCLASSIFIED (Limited Distribution).

[QIC 1988a] *Quadrilateral Technical Interface Design Plan, Version A.7*, Quadrilateral Interface Committee, 15 April 1988, UNCLASSIFIED (Limited Distribution).

[QIC 1988b] *Quadrilateral Test and Demonstration Management Plan*, Quadrilateral Interface Committee, 15 April 1988, UNCLASSIFIED (Limited Distribution).

[QIPMP 1993] *Quadrilateral Interoperability Programme Management Plan (QIPMP)*, Version B.0, LTC Theodor Hodoschal, OPM OPTADS (SFAE-CC-MVr-1), US Army CECOM, 9 December 1993, NATO UNCLASSIFIED.

[Radack 1993] "Industry/Government Open Systems Specification: The Development of GOSIP Version 3," Shirley M. Radack, *Federation Facts*, Summer 1993.

[Rannestad 1991] *Workshop on Conformance Testing*, A. Rannestad, NATO International Staff, DS(CCC-IP)(91)292, 7 June 1991, NATO UNCLASSIFIED.

[Rannestad 1994] Private communication with Dr. A. Rannestad, ICP Section, C3 Directorate, NATO International Staff, 25 January 1994, NATO UNCLASSIFIED.

[Rannestad 1994a] Private Communication on CNAD/TSGCE Restructuring, Dr. A. Rannestad, ICP Section, C3 Directorate, NATO Headquarters International Staff, 25 January 1994, NATO UNCLASSIFIED.

[Rannestad 1994b] Private Communication on STANAG Status, Dr. A. Rannestad, ICP Section, C3 Directorate, NATO Headquarters International Staff, 25 January 1994, NATO UNCLASSIFIED.

[Rash 1993] "APPS Take Flight," Wayne Rash, Jr., *Communications Week*, November 1, 1993.

[Rayner 1987] "OSI Conformance Testing," D. Rayner, *Computer Networks and ISDN Systems*, Volume 14, 1987.

[RDA 1990] *Proposed NWI: RDA Support for Stored DBL Statements*, SC21/WG3 N 1125, RDA SEL 24 (Rev 1), October 1990.

[Reed 1988] *Briefing to the 22nd ADSIA Plenary on STAMINA and QTIDP*, Annex W to ADSIA-RCX-DS/22, Rex Reed, NACISA, 17-21 October 1988, NATO UNCLASSIFIED.

[Reed 1990] *The STAMINA Specification*, J. R. Reed, S. Goldani, and N. Sanli, NACISA, Proceedings of the Military OSI Symposium, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[Reed 1991] *User-System Software Interface Standards: Issues and Prospects*, Paul Reed and Ken Holdaway, 1991.

[Reichlen 1990] *User Performance of Tactical Networks in the ITDN*, Gladys Reichlen and Allison Mankin, The MITRE Corporation, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[Rensselaer 1992] *Processing Tools for EXPRESS*, Peter R. Wilson, Rensselaer Design Research Center, Rensselaer Polytechnic Institute, Technical Report Number: 92003, February 1992.

[Reynolds 1987] *Assigned Numbers*, J. K. Reynolds, Request for Comments (RFC) 1010, DDN Network Information Center, SRI International, May 1987.

[Rigden 1991] *TSGCE SG9 (CSNI) Report of the Chairman (C. Rigden) to SG9*, 2 December 1991, NATO UNCLASSIFIED.

[RM 1989] *Information Processing Systems - Computer Graphics - Reference Model of Computer Graphics*, RM/20, Second Working Draft, 3 February 1989.

[RNLA 1994] Private Communication from the Royal Netherlands Army (RNLA), including excerpts from *EUCLID RTP 6.1-GRACE*, Volumes I and II, The GRACE Consortium, Steria (FR), 22 December 1993.

[Romann 1992] Private Communication from M. Romann, Section d'Etudes et Fabrications des Telecommunications (SEFT), Direction des Armements Terrestres/DGA, Ministere de la Defence, France, January 1992, NATO UNCLASSIFIED.

[Rose 1989] *The ISO Development Environment Users Manual*, Marshall T. Rose, The Wollongong Group, March 1989.

[Rose 1990] *The Open Book - A Practical Perspective on OSI*, Marshall T. Rose, Prentice Hall, Englewood Cliffs, New Jersey, 1990.

[Rothenhofer 1993] "ISDN in Public and Private Networks," Karl Rothenhofer, Alcatel SEL AG (Germany), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Rudderham 1994] Private Communication with COL Rudderham (MOD Canada), SHAPE Policy and Requirements Division (ACCS), 26 January 1994.

[SANISI 1989] *Security Architecture for NATO Information Systems Interconnection (SANISI) (NU), Version 2.0*, Ad Hoc Working Group on Security, TSGCE SG9, AC/302(SG/9)D/53, 14 April 1989, NATO CONFIDENTIAL.

[Savoye 1991] *Report of the US Representative (Dick Savoye) to the US SG9 Coordination Group*, 29 October 1991, NATO UNCLASSIFIED.

[SC6 N 6219 1990] *Liaison to SC21 on Lower Layer Security*, JTC1/SC6 N 6219, 4 October 1990.

[SC6 N 6887 1991] *Proposal for a New Work Item (NP): Enhanced Transport Mechanism (Technical Report - Type 3)*, JTC1/SC6, SC6 N 6887, 15 August 1991.

[SC6 N 6976 1991] *Request for SGFS Member Comment on Standardization of Profile Test Specifications*, ISO/IEC JTC1/SGFS, JTC1/SC6 N 6976, 10 September 1991.

[SC6 N 6977 1991] *The Way Ahead: Output Document from June 1991 SGFS Meeting*, ISO/IEC JTC1/SGFS, JTC1/SC6 N 6977, 10 September 1991.

[SC14 N 734 1993] *Secretariat's Report to ISO/IEC JTC1 Plenary Meeting in Washington, D.C., 1-4 February 1994*, SC14 Secretariat, November 1993.

[SC21 N 197 1982] *Concepts and Terminology for the Conceptual Schema and the Information Base*, TC97/SC5 N 695 and SC21 N 197, March 1982.

[SC21 N 236 1985] *Assessment Guideline for Conceptual Schema Language Proposals*, TC97/SC21/WG5-3, SC21 N 236, 31 August 1985.

[SC21 N 1927 1987] *Remote Database Access*, Tutorial, SC21 N 1927, SC21/WG3, 28 July 1987.

[SC21 N 2643 1988] *Remote Database Access*: SQL Specialization, SC21 N 2643, SC21/WG3, 9 May 1988.

[SC21 N 3134 1988] *Revised Report of the SC21 Strategic Planning Meeting*, SC21 N 3134, October 1988.

[SC21 N 3342 1989] *Information Processing Systems - Open Systems Interconnection - Remote Database Access*: SQL Specialization, Service and Protocol, SC21 N 3342, SC21/WG3, 26 January 1989.

[SC21 N 3885 1989] *UN/EDIFACT Information Pack*, SC21 N 3885, 19 September 1989.

[SC21 N 3925 1989] *Liaison Statement to JTC1 SC21 from JTC1 SWG-EDI*, JTC1 SWG-EDI, SC21 N 3925, 19 October 1989.

[SC21 N 3930 1989] *Liaison Statement from JTC1/SC18 to JTC1/SC21/WG5 on Comments on Terminal Management*, SC21 N 3930, SC18/WG4, 19 October 1989.

[SC21 N 4002 1989] *Extended Application Layer Structure*, ANSI Contribution to SC21/WG6, SC21 N 4002, 19 October 1989.

[SC21 N 4025 1989] *ODP: Working Document on Topic 8.1—Draft Basic Reference Model of Open Distributed Processing*, SC21 N 4025, 11 December 1989.

[SC21 N 4187 1989] *Issues on Upper Layers Conformance Testing*, SC21 N 4187, November 1989.

[SC21 N 4189 1989] *Comments on the Integration of X-Windows Into the OSI Environment*, SC21 N 4189, December 1989.

[SC21 N 4192 1989] *Proposed Document Type to Support CGM*, SC21 N 4192, SC21/WG5, December 1989.

[SC21 N 4195 1990] *Draft WG3 Position on Conceptual Schema Question*, SC21 N 4195, February 1990.

[SC21 N 4342 1990] *Liaison Statement from SC18 to SC21/WG5 on Conference Application New Study Item Including RODE*, SC21 N 4342, January 1990.

[SC21 N 4356 1990] *Terms of Reference and Plan of Action for the Reassessment of JTM Full Class*, SC21 N 4356, January 1990.

[SC21 N 4472 1990] *Liaison Statement from JTC1/SC18 to JTC1/SC21 on Changes to ASN.1*, SC21 N 4472, SC18/WG3 (title is in error—changes are for ODA, ISO 8613), 22 February 1990.

[SC21 N 4511 1990] *US Comments on Conceptual Schema*, SC21 N 4511, 15 March 1990.

[SC21 N 4520 1990] *Issues for Consideration by Joint ULA/ODP Meeting*, Seoul, May/June 1990, SC21 N 4520, Workshop on Distributed Applications, 18 April 1990.

[SC21 N 4523 1990] *Modelling of Application Program Interfaces and Remote Procedure Calls*, SC21 N 4523, 2 April 1990.

[SC21 N 4524 1990] *Consideration of the Data Management Component of Application Standards*, SC21 N 4524, Workshop on Distributed Applications, 23 April 1990.

[SC21 N 4526 1990] *Application Layer Security Considerations*, SC21 N 4526, 18 April 1990.

[SC21 N 4559 1990] *Liaison Statement of SC21 on OSI Reference Model Update Effort*, SC21 N 4559, CCITT SG VII, March 1990.

[SC21 N 4565 1990] *Liaison Statement to SC21/WG4/WG7 on Time Synchronization*, SC21 N 4565, CCITT SGVII, March 1990.

[SC21 N 4603 1990] *Position on Reassessment of JTM Full Class Protocol*, AFNOR, SC21 N 4603, March 1990.

[SC21 N 4641 1990] *US Position on JTM Reassessment*, SC21 N 4641, March 1990.

[SC21 N 4655 1990] *Reassessment of Project 1.21.44, Architectural Semantics for FDTs*, SC21 N 4655, 20 April 1990.

[SC21 N 4681 1990] *User Requirements for Multi-Party Communications (MPC)*, SC21 N 4681, Canada, May 1990.

[SC21 N 4759 1990] *USA Position on the Progression of DIS 10026*, SC21 N 4759, 12 March 1990.

[SC21 N 4767 1990] *US Response to SC21/WG6 N 7889 on Requirements for RPC Interface Definition Notation*, SC21 N 4767, 11 May 1990.

[SC21 N 4901 1990] *Second Working Draft for Amendment 1 to ISO 9545 ALS on Extended Application Layer Structure*, SC21 N 4901, SC21/WG6, June 1990.

[SC21 N 4911 1990] *Modelling for Communications Aspects of Distributed Applications*, SC21 N 4911, SC21/WG6, May 1990.

[SC21 N 4926 1990] *Liaison to CCITT SG VII(Q19) on OSI RPC*, SC21 N 4926, SC21/WG6, June 1990.

[SC21 N 4928 1990] *Remote Call Procedure Definitions and Requirements*, SC21 N 4928, SC21/WG6, June 1990.

[SC21 N 5002 1990] *Commencement of Work on Security ASEs*, SC21 N 5002, SC21/WG6, 31 May 1990.

[SC21 N 5014 1990] *Liaison Statement to CCITT SG VII (Q.23) on Collaborative Work on OSI Registration*, SC21 N 5014, 6 June 1990.

[SC21 N 5141 1990] *Proposal for Registration of Q3/002*, SC21 N 5141, SC21/WG3, 19 June 1990.

[SC21 N 5172 1990] *Combined Use of RPC and OSI TP*, SC21 N 5172, SC21/WG5 and SC21/WG6, June 1990.

[SC21 N 5184 1990] *Queued Data Transfer for TP*, SC21 N 5184, SC21/WG5, May 1990.

[SC21 N 5546 1990] *Agreement on Planning Future Releases of CMIS/P*, Collaborative OSI Systems Management Meeting, 12-16 November 1990, SC21 N 5546.

[SC21 N 5583 1991] *Report of the Liaison Meeting with SC22/WG11*, Amsterdam, September 1990, SC21 N 5583, 7 January 1991.

[SC21 N 5602 1991] *Proposed Liaison Between ISO TC 184/SC5/WG2 and ISO/IEC JTC1/SC21/WG4*, SC21 N 5602, 11 January 1991.

[SC21 N 5603 1990] *Rapporteur's Report of the DIS 100225 (TP) Editing Meeting*, San Francisco, 26 November to 14 December 1990, SC21 N 5603, 11 January 1990.

[SC21 N 5618 1991] *Working Document on ASN.1 - Part 1*: General, SC21 N 5618, 5 February 1991.

[SC21 N 5682 1991] *Contribution from JTC 1/SC 22/WG11, Binding Techniques for Languages*, SC21 N 5682, 5 February 1991.

[SC21 N 5851 1991] *USA Contribution to SC21 on the Conceptual Schema Topic*, SC21 N 5851, 4 April 1991.

[SC21 N 5997 1991] *USA Position on Use of RTSE by SC21 Standards*, SC21 N 5997, 12 June 1991.

[SC21 N 6012 1991] *Response to SC21 N 5759, Comment on Directory Implementor's Guide*, SC21 N 6012, May 1991.

[SC21 N 6066 1991] *Collection of Liaison Statements from SC21 to SC21*, SC21 N 6066, 4 December 1991.

[SC21 N 6067 1991] *Request for Comments on Requirements for Management in the Upper Layers of OSI*, SC21 N 6067, 2 July 1991.

[SC21 N 6085 1991] *Revised New Work Item on ODP Trader*, SC21 N 6085, SC21/WG7, 30 May 1991.

[SC21 N 6088 1991] *Proposal for a WG7 Question on the Suitability of the Formal Description Technique Z for Use in ODP*, May 1991.

[SC21 N 6130 1991] *Generic Transfer Syntax Providing Upper Layers Security*, SC21 N 6130, 15 July 1991.

[SC21 N 6158 1991] *Final Answer to Q1/62 (Quality of Service (QoS) Architectural Issues)*, SC21 N 6158, 22 July 1991.

[SC21 N 6159 1991] *NP for OSI - Quality -of-Service (QoS) Framework*, SC21 N 6159, 2 August 1991.

[SC21 N 6224 1991] *Proposed EDIFACT/FTAM Document Type*, SC21 N 6224, 3 July 1991.

[SC21 N 6225 1991] *Response to Liaison from JTC1/SC24/WG3 about CGM Document Types*, 3 May 1991, SC21 N 6225, 3 July 1991.

[SC21 N 6227 1991] *Virtual Terminal Support of ODA*, SC21 N 6227, 3 July 1991.

[SC21 N 6228 1991] *Liaison Statement on CCR to WG1 and WG6, FTAM Use of CCR*, SC21 N 6228, 3 July 1991.

[SC21 N 6229 1991] *Request for National Body Contributions on Document Type Registration*, SC21 N 6229, 3 July 1991.

[SC21 N 6230 1991] *On Conformance to Document Types*, SC21 N 6230, 3 July 1991.

[SC21 N 6251 1991] *Proposed New Question on the IRDS Definition Level Content Standard for Semantic Unification Meta Model (SUMM)*, SC21 N 6251, 23 July 1991.

[SC21 N 6252 1991] *Proposal for a NP: Revision of the IRDS Framework*, SC21 N 6252, 1 July 1991.

[SC21 N 6253 1991] *Proposed New Question on the Approach to Remote IRDS Access*, SC21 N 6253, 23 July 1991.

[SC21 N 6439 1991] *Liaison Statement to JTC1/SC21 on Enhanced Transport Mechanisms and Group NSAP Addressing*, SC6, SC21 N 6439, 1 October 1991.

[SC21 N 6449 1991] *Calling Notice for SC21 Special Meeting on Conceptual Schema Facilities and Common Data Modelling Facilities, 9-13 March 1992, Renesse, The Netherlands*, SC21 N 6449, 9 October 1991.

[SC21 N 6530 1992] *Report of the JTC1 Plenary Ad Hoc Group on EDI*, SC21 N 6530, 31 October 1991.

[SC21 N 6559 1991] *Liaison to SC21/WG4 Concerning Proposed Common Prioritization Work*, SC21 N 6559, 25 November 1991.

[SC21 N 6606 1992] *Collection of Liaison Statements from SC27 to SC21*, SC21 N 6606, May 1992.

[SC21 N 6614 1991] *SC21 Recommended Action to Address Problems of Data Modelling Standards Coordination*, SC21 N 6614, 17 December 1991.

[SC21 N 6656 1992] *Liaison Statement to SC21/WG6 on Compatibility of ROS and RPC*, SC21 N 6656, 7 January 1992.

[SC21 N 6664 1992] *Liaison Statement to SC22/WG15 on Software Management*, SC21 N 6664, 8 January 1992.

[SC21 N 6719 1992] *Recommendations of the CCITT and ISO Collaborative Interim Meeting Covering ROSE Enhancements*, SC21 N 6719, April 1992.

[SC21 N 6749 1992] *Proposal for a New Work Item on Information Technology - Text Communication - Coordinated Time Service in an OS' Environment*, SC18/WG4, SC21 N 6749, 20 February 1992.

[SC21 N 6798 1992] *USA Request for Extensions to ACSE*, SC2 N 6798, 26 March 1992.

[SC21 N 6802 1992] *Problems with Certifying FTAM Implementations as Conformant*, SC21 N 6802, 26 March 1992.

[SC21 N 6812 1992] *Request to Apply the Procedures for the Reactivation of the Multi-Peer Data Transmission (MPDT) Project*, SC21 N 6812, March 1992.

[SC21 N 6814 1992] *Liaison Statement to SC21 on Lower Layer Multicast Work*, SC21 N 6814, 31 March 1992.

[SC21 N 6819 1992] *Report of the ISO/IEC-CCITT Joint OSI Conformance Group Interim Meeting Held in Durham, North Carolina, 4-8 November 1991*, SC21 N 6819, 31 March 1992.

[SC21 N 6821 1992] *Internationalization of the Directory*, SC21 N 6821, March 1992.

[SC21 N 6892 1992] *Liaison Statement to SC21/WG4 on Atomic Transaction Interface*, SC21 N 6892, 4 May 1992.

[SC21 N 6894 1992] *Liaison Statement to Joint CCITT/ISO 9596-2/X.712 Editing Meeting*, 29 May 1992, Ottawa, SC21 N 6894, 4 May 1992.

[SC21 N 6896 1992] *Liaison Statement to Joint CCITT/ISO 10164-13/X.738 Editing Meeting, 29 May - 3 June 1992, Ottawa*, SC21 N 6896, 4 May 1992.

[SC21 N 6905 1992] *Liaison Statement to SC21/WG6: Report on Q26/VII Meeting*, April 1992, SC21 N 6905, 5 May 1992.

[SC21 N 6915 1992] *Liaison Statement to SC21 re Profiles for Systems Management Functions (10164-1 to -6) and Definition of Management Information (19165-2)*, SC21 N 6915, 6 May 1992.

[SC21 N 6945 1992] *Recommendations of the SC21 Special Meeting on Conceptual Schema Facilities/Common Data Modelling Facilities, Renesse, March 1992*, SC21 N 6945, June 9, 1992.

[SC21 N 6956 1992] *Status Report on CCITT Study Group Activities*, SC21 N 6956, June 9, 1992.

[SC21 N 6968 1992] *Request for Comment on Issues Concerning Upper Layer Management*, SC21 N 6968, 9 June 1992.

[SC21 N 6972 1992] *Draft Answer to Q6/2 - Relationship Between the OSI Upper Layer Architecture and ODP*, SC21 N 6972, May 1992.

[SC21 N 6974 1992] *Liaison Statement to SC6 Concerning a Request for Incorporation of New Protocol Information Attributes in ISO/IEC 9594-6/DAM1*, SC21 N 6974, 10 June 1992.

[SC21 N 6985 1992] *Request for Comments on Compression in Presentation Layer*, SC21 N 6985, 11 June 1992.

[SC21 N 7013 1992] *Proposed NP for Enhancements to ROSE Concepts, Model & Notation, ROSE Service Definition and Protocol Specification*, SC21 N 7013, 13 July 1992.

[SC21 N 7014 1992] *Proposed NP for Extensions to ACSE Covering ASOs and ASO-associations*, SC21 N 7014, 5 August 1992.

[SC21 N 7051 1992] *Proposed Draft Answer to Question Q7/1 on the Suitability of the Formal Description Z for Use in ODP*, May 1992.

[SC21 N 7062 1992] *Liaison Statement to SC6 on Multipeer Data Transmission*, SC21 N 7062, May 1992.

[SC21 N 7063 1992] *Liaison Statement to CCITT SG VII on Multipeer Data Transmission*, May 1992.

[SC21 N 7069 1992] *Draft Answer to Q1/49.9 on Long-term Solution to General and Dependent Conformance*, ISO/IEC JTC1/SC21/WG1 Meeting, Ottawa, May 1992, 22 July 1992.

[SC21 N 7073 1992] *Proposed New Sub-Question Q1/49.9 on Long-Term Solution to General and Dependent Conformance*, ISO/IEC JTC1/SC21/WG1 Meeting, Ottawa, May 1992, 22 July 1992.

[SC21 N 7079 1992] *Working Draft Answer to Q1/63.2 on Testability of Managed Objects*, SC21/WG1 Meeting, Ottawa, May 1992, 7 October 1992.

[SC21 N 7088 1992] *Proposed New Question Q1/66 on ODP Conformance Testing Methodology*, JTC1/SC21/WG1 Meeting, Ottawa, May 1992, 22 July 1992.

[SC21 N 7089 1992] *Statement on Scope and Usability of the Security Frameworks for Open Systems*, SC21/WG1, SC21 N 7089, May 1992.

[SC21 N 7090 1992] *Proposed New Question Q1/65 on User Requirements for OSI Systems Supporting Time Critical Communications*, ISO/IEC JTC1/SC21/WG1 Meeting, Ottawa, May 1992, 22 July 1992.

[SC21 N 7094 1992] *Draft Answer to Question Q1/68 on the Definition of the Term "Application-Process-Title" in the OSI Reference Model*, SC21 N 7094, 22 July 1992.

[SC21 N 7096 1992] *Draft Answer to Q1/48.6 - Enhancements to LOTOS*, ISO/IEC JTC1/SC21/ WG1 Meeting, Ottawa, May 1992, 22 July 1992.

[SC21 N 7098 1992] *Proposed New Question Q1/69 on Conformance Assessment for OSI Security*, ISO/IEC JTC1/SC21/WG1 Meeting, Ottawa, May 1992, 22 July 1992.

[SC21 N 7105 1992] *Reply and Disposition of Comments on NP on Development of Enhanced Functionality for CMIS/P (JTC1 N 1667)*, ISO/IEC JTC1/SC21/WG4 Meeting, Ottawa, May 1992, 5 August 1992.

[SC21 N 7107 1992 rev] *Reply and Disposition of Comments on NP on Development of Enhanced Functionality for CMIS/P (JTC1 N 1667)*, ISO/IEC JTC1/SC21/WG4 Meeting, Ottawa, May 1992, 5 August 1992.

[SC21 N 7116 1992] *Working Document on Complex Attribute Types*, SC21 N 7116, 3 July 1992.

[SC21 N 7117 1992] *Request for National Body Input on Principles of Conformance for Managing Systems*, SC21 N 7117, 3 July 1992.

[SC21 N 7129 1992] *Request for National Body Contributions to Progress Work Item on Distributed Management*, SC21 N 7129, 3 July 1992.

[SC21 N 7134 1992] *Preliminary Document on Multiple Input Metric Object*, ISO/IEC JTC1/SC21/WG4 Meeting, Ottawa, May 1992, 21 July 1992.

[SC21 N 7140 1992] *Reply to Liaison Statement for CCITT SG VII Regarding the Comments on Notational Tools in SC21 N 6568*, SC 21 N 7140, 9 July 1992.

[SC21 N 7145 1992] *Liaison Statement to SC21/WG1, SC21/WG6 (8), SC6 and SC27 on Security Requirements for Systems Management*, SC21 N 7145, May 1992.

[SC21 N 7146 1992] *Liaison Statement to SC22/WG15 on Software Management*, SC21 N 7146, 28 May 1992.

[SC21 N 7162 1992] *Status of Project JTC1.21.12.08.02, FTAM Virtual Filestore Service Enhancements*, SC21 N 7162, June 1992.

[SC21 N 7175 1992] *Liaison Statement to SC6 on Requirement for Non-Blocking Transport Expedited Service*, SC21 N 7175, 9 July 1992.

[SC21 N 7178 1992] *Proposed NP for Guidelines for the Design of IRDS Content Modules*, SC21 N 7178, July 13, 1992.

[SC21 N 7181 1992] *Proposed Draft Answer to Q3/009 - Approach to Remote IRDS Access*, JTC1/SC21/WG3 Meeting, Ottawa, May 1992.

[SC21 N 7204 1992] *Resolutions of the Eighth Plenary Meeting of ISO/IEC JTC1/SC21, 2-3 June 1992, Ottawa, Canada*, SC21 N 7204, Revised 8 June 1992.

[SC21 N 7208 1992] *Proposal for an SC21 Special Working Group (SWG) on Modelling Facilities*, SC21 N 7208, June 10, 1992.

[SC21 N 7360 1992] *Development of the SGFS Procedures to Cover Other TCs and the Open System Environment (SGFS N 590)*, SC21 N 7360, September 1992.

[SC21 N 7417 1992] *Association Management Concepts*, SC21/WG8 TP Association Pool Rapporteur Group Meeting in Berlin, October 1992, SC21 N 7417, 3 November 1992.

[SC21 N 7424 1992] *Rapporteur's Report on the First API Study Group Meeting*, SC21 N 7424, 17 November 1992.

[SC21 N 7443 1992] *Summary of Voting on SC21 N 6984, Proposed NP for Class of Mappings from a Single ASN.1 Type to an FTAM Document Type*, SC21 N 7443, 20 November 1992.

[SC21 N 7467 1992] *Summary of Voting on SC21 N 7290, Proposed New Question Q1/65 on User Requirements for OSI Systems Supporting Time Critical Communications*, SC21 N 7467, 23 November 1992.

[SC21 N 7471 1992] *Summary of Voting on SC21 N 7078, Draft Answer to Q1/49.8 - Conformance and Registration*, SC21 N 7471, 24 November 1992.

[SC21 N 7473 1992] *Summary of Voting on SC21 N 7098, Proposed New Question Q1/69 on Conformance Assessment for OSI Security*, SC21 N 7473, 24 November 1992.

[SC21 N 7476 1992] *Summary of Voting on SC21 N 7088, Proposed New Question Q1/66 on ODP Conformance Testing Methodology*, SC21 N 7476, 24 November 1992.

[SC21 N 7483 1992] *Proposal for a New Work Item on Mapping of the OSI System Management - Object Management Function onto Message Handling Systems (MHS)*, SC21 N 7483, 1 December 1992.

[SC21 N 7487 1992] *Report of the Inter-Agency edi Working Group Meeting*, 5-6 October 1992, Geneva, SC21 N 7487, 7 December 1992.

[SC21 N 7490 1992] *Information Regarding the CCITT's Electronic Information Exchange - TELEDOC*, CCITT, SC21 N 7490, 7 December 1992.

[SC21 N 7534 1993] *Liaison Statement to System Management Functions - Performance Management Group on Need for ICS for ISO/IEC 10164-11*, 25 February 1993.

[SC21 N 7535 1993] *Liaison Statement to System Management Functions - Performance Management Group on New Work for Amendment to ISO/IEC 10164-11*, 25 February 1993.

[SC21 N 7542 1993] *Overview of Namur Output Documents (SWG-MF Study Period)*, SC21 N 7542, 2 February 1993.

[SC21 N 7577 1993] *Multiple Liaison Statement to SC21 on Various Topics*, Interim Meeting of CCITT SG VII, Geneva, 26-30 October 1992, SC21 N 7577, 15 January 1993.

[SC21 N 7579 1993] *Summary of Voting on Document JTC1 N 2039, Proposal for a New Work Item: Internationalization of the Directory*, SC21 N 7579, 15 January 1993.

[SC21 N 7580 1993] *Summary of Voting on Document JTC1 N 2040, Proposal for a New Work Item: Authentication and Related Security Services for Distributed Applications*, SC21 N 7580, 15 January 1993.

[SC21 N 7587 1993] *Liaison Statement to SC18/WG4 Regarding Time Management Function*, SC21 N 7587, 27 January 1993.

[SC21 N 7588 1993] *Liaison Statement to CCITT Q24/VII Concerning the Use of Formal Techniques for the Specification of Managed Objects*, SC21 N 7588, 27 January 1993.

[SC21 N 7613 1993] *Request for a Liaison Between the Object Management Group (OMG) and the ISO/IEC JTC1/SC21/WG7*, 23 February 1993.

[SC21 N 7614 1993] *Mechanism of the Mapping Between ISN and ASN.1*, SC21 N 7614, 4 February 1993.

[SC21 N 7630 1993] *Call for Input on Work Plan for SC21/WG4 Systems Management*, SC21 N 7630 1993, 2322 February 1993.

[SC21 N 7642 1993] *Liaison Statement to SC21 on the PREMO Project*, 24 February 1993.

[SC21 N 7643 1993] *Liaison Statement to SC 21 Regarding the Suitability of the Packed Encoding Rules for Encoding the IPI-IIF*, 24 February 1993.

[SC21 N 7651 1993] *Request for S-liaison Between the EWOS/EG DBE and ISO/IEC JTC1/SC21/WG3*, 5 March 1993.

[SC21 N 7676 1993] *Initial Abstract Test Suite for TP*, SC21 N 7676, 15 March 1993.

[SC21 N 7696 1993] *Liaison Statement to SC21 on Multipeer Data Transmission (MPDT)*, SC6/WG4, SC21 N 7696, 29 March 1993.

[SC21 N 7713 1993] *Resolutions of the ISO/IEC JTC1 Plenary Meeting*, 23-26 March 1993, Berlin, Germany, SC21 N 7713, 5 April 1993.

[SC21 N 7720 1993] *Revised Title and Scope for SC21*, SC21 N 7720, 8 April 1993.

[SC21 N 7723 1993] *Summary of Voting on Document JTC1 N 2264, Proposal for a New Work Item: Extensions to ACSE Covering ASOs and ASO-Associations*, SC21 N 7723, 19 April 1993.

[SC21 N 7728 1993] *Proposals for Re-assessment or Cancellation of Specific SC21 Projects*, SC21 N 7728, 6 April 1993.

[SC21 N 7742 1993] *Summary of Voting on Document JTC1 N 2247, Proposal for a New Work Item: Guidelines for the Design of IRDS Content Modules*, SC21 N 7742, 19 April 1993.

[SC21 N 7744 1993] *Summary of Voting on Document JTC1 N 2265 Proposal for a New Work Item: SQL Multimedia and Application Packages (SQL/MM)*, SC21 N 7744, 19 April 1993.

[SC21 N 7764 1993] *Confirmation of ISO 9807: 1987*, SC21 N 7764, 27 April 1993.

[SC21 N 7817 1993] *Requirement for Timely Progression of the Application Guidelines*, SC21 N 7817, May 1993.

[SC21 N 7845 1993] *Internet Structure and Working Group Summary*, SC21 N 7845, 1 June 1993.

[SC21 N 7866 1993] *Enhancements of Efficiency for SC21 Protocols*, SC21 N 7866 1993, 7 June 1993.

[SC21 N 7868 1993] *Progression of ACSE Texts*, SC21 N 7868, 8 June 1993.

[SC21 N 7915 1993] *Liaison Statement to SC6 in Reply to SC6 N 7961 and 7614*, SC21/WG8, August 1993.

[SC21 N 7980 1993] *Liaison Statement to ITU-TS/SG15 on Change Over Function*, August 1993.

[SC21 N 7992 1993] *Liaison Statement to ISO/TC184/SC5/WG2 Concerning Activity on Quality of Service*, SC21/WG1, August 1993.

[SC21 N 8003 1993] *NP on Architecture for Multipeer Data Communications*, June 1993.

[SC21 N 8010 1993] *Open Systems Assessment Methodology*, June 1993.

[SC21 N 8018 1993] *Liaison Statement to ITU-TS SG7 (Q19/7) on Q1/65.2—OSI Protocols Efficiency*, August 1993.

[SC21 N 8019 1993] *Liaison Statement to ITU-TS/SG7 on Q1/67 - Generalization of ASO Concept*, SC21/WG1, August 1993.

[SC21 N 8034 1993] *Liaison Statement to the Object Management Group*, SC21/WG7, August 1993.

[SC21 N 8043R 1993] *SC21/WG4 Convener's Report to the SC 21 Plenary Meeting, June 1993, Yokohama, Japan*, SC21 N 8043R, 12 July 1993.

[SC21 N 8045 Revised 1993] Report of the SC21 Study Group on APIs, June 1993.

[SC21 N 8057 1993] *Recommendation to Progress Work on the Use of Standard Data Modelling Facilities in the Preparation of International Standards*, SWG-MF, July 1993.

[SC21 N 8081 1993] *Resolutions of the Ninth Plenary Meeting of ISO/IEC JTC1/SC 21, 29-30 June 1993, Yokohama, Japan*, SC21 N 8081.

[SC21 N 8082 1993] *ISO/IEC JTC1/SC21 Programme of Work*, SC21 N 8082, 28 October 1993.

[SC21 N 8103 Revised 1993] *Request from SC21 to JTC1 Concerning the "Fast Tracking" of the PCTE Document*, June 1993.

[SC21 N 8109 1993] *Proposed New Question Q3/011, "Harmonization of Client/Server Capabilities,"* SC21/WG3, SC21 N 8109, September 1993.

[SC21 N 8123 1993] *Resolutions of the SC21/WG3 Meeting, 15-25 June 1993, Yokohama*, SC21 N 8123 1993, 22 September 1993.

[SC21 N 8127 1993] *Liaison Information on Modelling Facility Interim Work*, SC21 SWG-MF, June 1993.

[SC21 N 8202 1993] *Working Draft on IRDS Services Interface Extensions*, September 1993.

[SC21 N 8205 1993] *SQL Multimedia and Hypermedia Application Packages (SQL/MM) Project Plan (Revised)*, SC21/WG3, September 1993.

[SC21 N 8262 1993] *Liaison Statement to SC21 and SC6 on OSI Quality of Service*, ITU-TS SG7, October 1993.

[SC21 N 8263 1993] *Liaison Statement to SC21 and SC6 on OSI Quality of Service Framework Specifications*, ITU-TS SG7, October 1993.

[SC21 N 8267 1993] *Liaison Statement to SC21 on OSI Multicast Architecture*; ITU-TS SG7, October 1993.

[SC21 N 8280 1993] *Liaison Statement to SC21/WG4 on Requirements and Directions for the Use of Formal Description Techniques for the Specification of Managed Objects*, ITU-TS SG7, October 1993.

[SC21 N 8282 1993] *Calling Notice and Draft Agenda for the Interim Meeting of the SC21/WG3 Rapporteur Group on Conceptual Schema Modelling Facilities, Aix en Provence, 17-21 January 1994*, October 1993.

[SC21 N 8305 1993] *A Data Modelling Facility: JDMF/MODEL-1992*, Japan, October 1993.

[SC21 N 8316 1993] *Comments on Standardized Programmatic Interfaces*, USA, October 1993.

[SC21 N 8320 1993] *UK Position on Programmatic Interface Standardization*, UK, November 1993.

[SC21 N 8321 1993] *Requirement for Partial Rollback*, USA, November 1993.

[SC21 N 8355 1993] *Liaison Statement to SC21/WG1 and SC22/WG15 on Conformance Testing*, December 1993.

[SC21 N 8380 1993] *Guide to Open System Security*, Working Draft Technical Report, December 1993.

[SC21 N 8384 1993] *Liaison Statement to SC21/WG1 on Multi-Peer Data Transmission*, ISO/TC184/SC5/WG2, December 1993.

[SC21 N 8385 1993] *Final Draft Version of TCCA Technical Report (DTR 12178) Sent to the ISO Central Secretariat for Publication*, ISO/TC184/SC5/WG2, December 1993.

[SC21 N 8397 1993] *Outline Contribution to Future Work as Proposed in SC21 N 8045 Rev 2*, SC21 SWG-SPI Meeting 8-11 November 1993 in Torina, January 1994.

[SC21/WG1 N 1140 1992] *UK Discussion Paper on Conformance Testing for OSI Security*, SC21/WG1 N 1140, March 1992.

[SC21/WG1 N 1156 1992] *Clarification on Use of the PICS*, SC21/WG1, N 1156, April 1992.

[SC21/WG1 N 1157 1992] *Contributions on LOTOS Enhancements*, JTC1/SC21/WG1 N 1157, April 1992.

[SC21/WG1 N 1233 1993] *Manager Role Conformance*, February 1993.

[SC21/WG3 N 1272 1991] *Guidelines for the Design of IRDS Content Modules*, SC21/WG3 N 1272, 1991.

[SC21/WG3 N 1279 1991] *Report of Meeting CDIF/1175/PDES Information Coordination*, 1-2 November 1991, SC21/WG3 N 1279.

[SC21/WG3 N 1283 1992] *IRDS Services Interface Extensions - Design Document*, JTC1/SC21/WG3 N 1283, 27 February 1992.

[SC21/WG3 N 1298 1992] *New Project Proposal: SQL ADT Packages*, SC21/WG3 N 1298, 3 April 1992.

[SC21/WG3 N 1345 1992] *Letter to Convenor, Government Telecommunications Agency/VPD, Ottawa Canada, EWOS, Expert Group on Database Enquiry*, SC21/WG3 N 1345, 1992.

[SC21/WG3 N 1371 1992] *Discussion between JTC1 SC21/WG3 and ISO TC 184/SC5/WG4*, 11 May 1992, SC21/WG3 N 1373.

[SC21/WG3 N 1406 1992] *Agreed Scope of Work for the Revision of the IRDS Framework (IS 10027)*, Ottawa, May 1992.

[SC21/WG3 N 1430 1992] *DBL Status Report*, 23 June 1992.

[SC21/WG3 N 1450 1992] *Proposed Structure of SQL3*, 20 November 1992.

[SC21/WG3 N 1452 1992] *DBL Liaison to CLID re: Tables*, 20 November 1992.

[SC21/WG3 N 1557 Revised 1993] *Proposal for the Registration of Q3/010: ODP and Distributed Database Systems*, June 1993.

[SC21/WG3 N 1644 1993] *Technical Report on the Semantic Unification of Meta-Model*, Volume 1, *Semantic Unification of Static Models*, US National Body, November 1993.

[SC21/WG3 N 1645 1993] *Knowledge Interchange Format (KIF)*, US National Body, November 1993.

[SC21/WG4 1989] *Liaison Statements to SC21/WG4*, SC21 N 3851-3853, 30 August 1989.

[SC21/WG4 N 1438 1992] *UK Contribution to 21/63.2, Testability of Managed Objects*, SC21/WG4 N 1438, March 1992.

[SC21/WG4 N 1451 1992] *Comments on SC21 N 6749: NP Time Services in an OSIE*, SC21/WG4 N 1451, 22 April 1992.

[SC21/WG4 N 1472 1991] *US Response to SC21 N 6679, Request for National Body Comments on the Progression of an Amendment to ISO/IEC 10164-11 on the Definition of Multiple Input Metric Objects*, SC21/WG4 N 1472, 7 March 1991.

[SC21/WG4 N 1527 1992] *Closing WG4 Plenary Report on Directory Meeting*, Ottawa, ISO/IEC/JTC1/SC21/WG4, 19-27 May 1992.

[SC21/WG4 N 1615 1992] *Report of the ISO/IEC JTC1 - CCITT Collaborative Meeting on Systems Management*, December 7-11, 1992, Eastbourne, UK., SC21 WG4 N 1615, 11 December 1992.

[SC21/WG4 N 1640 1992] *Proposed Amendment to GDMO*, SC21 WG4 N 1640, 11 December 1992.

[SC21/WG4 N 1641 1992] *Issues for Extended Systems Management Architecture (WG4 SD 1)*, SC21/WG4 N 1641, 11 December 1992.

[SC21/WG5 N 673 1992] *Minutes of the TP Group Meeting*, Ottawa, 21-29 May 1992, SC21/WG5 N 673, June 1992.

[SC21/WG6 N 1155 1992] *Provision of Guidance on Application of XALS Concepts*, SC21/WG6 N 1155, 1992.

[SC21/WG6 N 1158 1992] *Strawman Generic Security ESO-OSI Abstract Interface*, SC21/WG6 N 1158, 20 April 1992.

[SC21/WG6 N 1159 1992] *Proposal for a New Work Item on a Class of Mappings from a Single ASN.1 Type to an FTAM Document Type*, SC21/WG6 N 1159, 20 April 1992.

[SC21/WG6 N 1170 1992] *Comments on SC21 N 6656*, SC21/WG6 N 1170, 20 April 1992.

[SC21/WG6 N 1171 1992] *ASN.1 Information Objects, Constraints, Parameterisation - Tutorial and Worked Examples*, D. A. Steedman, Editor, SC21/WG6 N 1171, 20 April 1992.

[SC21/WG7 N 737 1992] *Report on the Joint Meeting of ISO/IEC JTC1/SC21/WG7 and SGVII.Q16 (ODP) on ODP Trader, Boulder, USA, 2-10 November 1992*, 27 November 1992.

[SC21/WG7 N 783 1993] *An Integrated Approach to Trader Contexts*, August 1993.

[SC21/WG7 N 811 1993] *Relations of Formal Descriptions of Different ODP Viewpoint Models*, August 1993.

[SC21/WG7 N 823 1993] *Joint Action Plan SC21/WG7 and WG7-ITU-TS/Q16/7 (ITU-TS Format)*, August 1993.

[SC21/WG7 N 836 1993] *Liaison Contributions for SC21/WG7*, SC21/WG3, August 1993.

[SC21/WG7 N 852 1993] *Outline of Information Specification for ODP Trader*, Australia, October 1993.

[SC21/WG8 N 62 1992] *Proposed Liaison Statement to SC22/WG11 on Internationalization and Reserved Words in Programming Language Standards*, SC21/WG8 N 62, 4 December 1992.

[SC21/WG8 N 63 1992] *Use of FTAM by Other ASEs Such as Directory*, SC21/WG8 N 63 1993, 4 December 1992.

[SC21/WG8 N 72 1993] *Future of TP Dialogue Recovery and Heuristic Decisions Projects*, SC21/WG8 N 72, 14 January 1993.

[SC21/WG8 N 82 1993] *TP Commitment Optimizations - Meeting Recommendations*, 25 February 1993.

[SC24 N 744 1992] *Concerning the Use of ASN.1 in the Image Processing and Interchange Image Interchange Facility (IPI-IIF) Standard*, SC21 N 744, 25 February 1992.

[Schneider 1990] "Standardization of Digital Geographic Data," Jan S. Schneider, Defense Mapping Agency, *Geo'89 Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[Schoka 1994] Private Communication on Status of POSIX with Andy Schoka, MITRE Corporation, Joint and Defense-Wide Systems, 21 March 1994, UNCLASSIFIED.

[Schultz 1990] *Report of the TSGCE Subgroup 9 on Data Processing and Distribution Meeting Held 9-11 May 1990*, US Representative (O. Schultz), May 1990, NATO UNCLASSIFIED.

[Schutzer 1987] *Artificial Intelligence: An Applications-Oriented Approach*, Daniel Schutzer, Van Nostrand Reinhold Company, 1987.

[SD-7 1992] *Issues List for Future Development of ISO/IEC TR 10000*, SGFS Standing Document SD-7, ISO/IEC JTC1/SGFS/N763, SC21 N 7830, December 1992.

[SDIO 1991] *Fixed and Mobile Segment (FMS) Standard*, Prepared by GE Aerospace for SDIO, CDRL A122, 17 December 1990, UNCLASSIFIED.

[Serrano 1994] Private Communication from MAJ Ernesto Serrano, Cuartel General de Tierra, Estado Mayor del Ejercito, Division de Operaciones, Spain, 18 February 1994, NATO UNCLASSIFIED.

[SG9/WG1 1990a] *Report to SG/9 by the Chairman of Working Group 1 on the 18th Meeting Held 26 February to 2 March 1990*, WG/1, 21 April 1990, NATO UNCLASSIFIED.

[SG9/WG1 1990c] *Report to SG/9 by the Chairman of Working Group 1 on Liaison with WG/2*, WG/1, 21 April 1990, NATO UNCLASSIFIED.

[SG9/WG2 1989] *Report to AC/302 SG/9 on WG/2 Activities (Brussels, October 1989)*, WG/2, 8 October 1989, NATO UNCLASSIFIED.

[SGFS 1989] *PAGODA Comments on DTR 10000-2 and Proposed FOD Taxonomy*, SGFS N 156, 6 November 1989.

[SGFS N 100 1992] *Framework and Taxonomy of International Standardized Profiles - Directory of ISPs and Profiles Contained Therein*, ISO/IEC JTC1/SGFS N 100, Rev. 4, 26 February 1992, p. 7.

[SGFS N 100 1992a] *Framework and Taxonomy of International Standardized Profiles - Directory of ISPs and Profiles Contained Therein*, ISO/IEC JTC1/SGFS N 100, Rev. 4, 26 February 1992, p. 9.

[SGFS N 242 1991] *Five-Year Meeting Schedule for JTC1/SGFS Plenary Meetings*, SGFS N 242.

[SGFS N 282 1991] *Resolutions of the 4th RWS-CC Meeting*, 18-19 October 1990, SGFS N 282, 17 January 1991.

[SGFS N 293 1991] *SGFS Report of the Secretariat*, SGFS N 293, January 1991.

[SGFS N 294 1991] *Issues List - Items for Future Developments of ISO/IEC TR 10000-1, TR 10000-2, and SGFS N 201, SGFS N 230, 7 February 1991; Draft Agenda and Hotel Information for the 7th ISO/IEC JTC1/SGFS Meeting*, SGFS N 294, 12 February 1991.

[SGFS N 295 1991] *Report of the Chairman to JTC1 Advisory Group*, SGFS N 295, 12 February 1991.

[SGFS N 1065 1993] *US Comments on OIW Liaison Statement to SGFS and EWOS/EG-OSE*, August 1993.

[SGFS N 1089 1993] *White Paper on OSE Profiling Concepts*, SGFS, SGFS N 1089, December 1993.

[SGFS N 1090 1993] *Liaison Statement to JTC1 on the Subject of PAS and APIs*, December 1993.

[SGFS N 1099 1993] *Draft Minutes of the SGFS Authorized Subgroup Meeting in Amsterdam, 29 November to 3 December 1993*, SGFS, December 1993.

[SGFS SD-7 1993] *Issues List for Future Development of ISO/IEC TR 10000*, SGFS N 1023, SGFS SD-7, September 1993.

[Shalikashvili 1993] Letter to LtGen Peter A. Kind, Director of Information Systems for Command, Control, Communications, and Computers, 3050/SHPRC/93, General John M. Shalikashvili, Supreme Allied Commander, Europe, SHAPE, 19 October 1993, NATO UNCLASSIFIED.

[SHAPE 1985] *Data Management Standardization for ACE ACCIS*, TM-776, SHAPE Technical Centre, July 1985, NATO UNCLASSIFIED.

[SHAPE 1988] *ACE Manual 96-1-4, Data Management*, SHAPE, 30 October 1988, NATO UNCLASSIFIED.

[SHAPE 1989] *An Architecture Based on OSI Principles for NATO Tactical Data Links*, TM-864, SHAPE Technical Centre, July 1989, NATO UNCLASSIFIED.

[SHAPE 1994] Private Communication from SHAPE ACOS-INT on Battlefield Information Collection and Exploitation Systems (BICES), Assistant Chief of Staff for Intelligence, SHAPE, 24 January 1993, NATO UNCLASSIFIED.

[Shirey n.d.] *Defense Data Network Security*, R. W. Shirey, US Defense Communications Agency, Undated.

[SILS 1989] *Standard for Interoperable LAN Security (SILS)*, P802.10/D1, IEEE, 6 January 1989.

[Singh 1992] *Harmonization of 2167A and 7935A*, Dr. Raghu Singh, DC SIG Ada Meeting, McLean Hilton, Tysons Corner, VA, August 19, 1992.

[Slone 1991] "Assessing LAN Technologies," John P. Slone, *Handbook of Local Area Networks*, John P. Slone and Ann Drinan, Editors, Auerbach Publishers, 1991.

[Sluman 1993] "Quality of Service—The Holy Grail or a Waste of Time?," Chris Sluman, Open-IT Limited (United Kingdom), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[SPACECOM 1991] *Assured Mission Support Space Architecture*, JTC3A Architecture Review, SPACECOM/J5J (LtCol O'Brien, Space Systems), 19 September 1991, UNCLASSIFIED.

[SPAG 1987] *Guide to the Use of Standards*, Version 3, Standards Promotion and Applications Group, January 1987.

[SPARTA 1991] *DoD Multicast Transport Service Specification*, SPARTA, Inc., for the Defense Communications Engineering Center of the Defense Information Systems Agency, 31 January 1991, UNCLASSIFIED.

[Spivey 1989] *The Z Notation*, J. M. Spivey, Prentice Hall, 1989.

[Stahl 1993] "Middleware," Stephanie Stahl, *Information Week*, November 1, 1993, pp. 62-68.

[Stallings 1985] *Computer Communications: Architecture, Protocols and Standards*, William Stallings, IEEE Computer Society Press, Silver Spring, MD, 1985.

[Stallings 1987] *Handbook of Computer-Communications Standards*, William Stallings, Volume 1: *The Open Systems Interconnection (ISO) Model and OSI-Related Standards*, Howard W. Sams and Company, 1987.

[Stallings 1987a] *Handbook of Computer-Communications Standards*, 3 Volumes, William Stallings, Howard W. Sams and Company,, 1987.

[Stallings 1991] *Data and Computer Communications*, William Stallings, Third Edition, MacMillan, Publishing Company, New York, 1991.

[Stallings 1993] *Networking Standards: A guide to OSI, ISDN, LAN, and MAN Standards*, William Stallings, Addison-Wesley Publishing Company, 1993.

[Stallings 1993a] "SNMPv2 Versus CMIP," William Stallings, *OSN: The Open Systems Newsletter*, Volume 7, Issue 4, April 1993, pp. 1-7.

[STAMINA 1990] *Standard Automated Message Interface for NATO ACCIS (STAMINA), Version 4.0*, April 1990.

[STAMINA 1990a] *The STAMINA Specification*, J. R. Reed, S. Goldani, and N. Sanli, NACISA, Proceedings of the Military OSI Symposium, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[STANAG 4406] *Military Message Handling System*, Review 1991], Draft STANAG 4406, 16 September 1991, NATO UNCLASSIFIED.

[Staton 1991] *Report to the Ad Hoc Working Group on Security to the SG9 Coordination Group*, Hal Staton, Chairman of the AHWG on Security, 29 October 1991, NATO UNCLASSIFIED.

[Staton 1994] Private Communication with Hal Staton, 4 February 1994.

[STC 1991] *NATO ISDN—Standards and Protocols*, Paper Submitted to SG9/WG2, 3 October 1991, SHAPE Technical Centre, NATO UNCLASSIFIED.

[STC 1991a] *Headquarters Information Systems (HIS) and ACCIS Testbed Laboratories*, Briefing to the ATCCIS Permanent Working Group, 8 April 1991, SHAPE Technical Centre Information Systems Division, NATO UNCLASSIFIED.

[STC TN-444 1993] *Recommendations for ACE Data Administration*, Draft Version 1.2, STC Technical Note TN-444, 1993, NATO UNCLASSIFIED.

[STDN-4 1993a] *Demonstration Plan for Secure Tactical Data Network-4 Demonstration*, 15 July 1993, UNCLASSIFIED.

[STDN-4 1993b] *Secure Tactical Data Network - Phase 4—Global Interoperability for the Warrior C4I*, Briefing Book, August 1993, UNCLASSIFIED.

[Steele 1984] *Common LISP*, G. L. Steele, Digital Press, 1984.

[STEI 1990] "Definition of Real-Time Services for the OSI Transport Layer," Pascal Prophete, STEI, French MOD, *Proceedings of the SHAPE Technical Centre Military OSI Symposium*, 6-8 June 1990, NATO UNCLASSIFIED.

[Stene 1990] "The North Sea Project," Ovind Stene, Norwegian Hydrographic Service, *Geo'89 Symposium on Geographical Information Systems for Command and Control*, 2-6 October 1989 at the SHAPE Technical Centre, Symposium Proceedings 6, Volume 1 (Unclassified Papers), SHAPE Technical Centre, The Hague, March 1990, NATO UNCLASSIFIED.

[Stewart 1994] Private Communication from Wing Commander Stewart on Air Command and Control System (ACCS), WGCDR Graham Stewart (UK-AF), SHAPE Policy and Requirements Division, Requirements and Programmes Branch, ACCS Section, 26 January 1994, NATO UNCLASSIFIED.

[Stoffel 1989] "DEC Opens an X Window for Control Systems," J. M. Stoffel, *Control Engineering*, Volume 36, Number 4, April 1989.

[Stollenmayer 1993] "Exploiting Public ISDNs for NATO," Peter Stollenmayer, SHAPE Technical Centre (The Netherlands), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Stone 1993] *Keeping you Informed*, Memo to OMG Board of Directors from Christopher Stone, Object Management Group, 9 September 1993.

[Strobel 1993] "ISDN-Communications Network for the German Armed Forces," Gunther Strobel, Alcatel SEL AG (Germany), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Sullivan 1992] *SQL Status: Standards and Validation Testing*, Joan M. Sullivan, NIST, NIST Users' Forum on APP and OSE, May 14, 1992.

[SUMM 1992] *Technical Report on the Semantic Unification Meta-Model*, Volume 1, *Semantic Unification of Static Models*, Dictionary/Methodology Committee of the IGES/PDES Organization (IPO), October 1992 (included in SC21/WG3 N 1644).

[SUN 1990] *Open Look Graphical User Interface: Application Style Guidelines*, Sun Microsystems, 1990.

[Sutherland 1993] "DRA Submarine Communications and Management Study (SCAMS)," Andrew D. Sutherland and David J. Bowley, Defence Research Agency-Naval Communications Division (United Kingdom), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Swanson 1991] *Software Product Specification for the Group-Oriented Transport Service Protocol*, John Swanson, SPARTA, Inc., for the Defense Communications Engineering Center of the Defense Information Systems Agency, 5 February 1991, UNCLASSIFIED.

[SWG-EDI 1991] *Report of the Special Working Group on a Conceptual Model for Electronic Data Interchange Standards and Services (SWG-EDI)*, ISO/IEC JTC1/SC21 N 5635, 23 January 1991.

[TA 1991] *Guide to IT Standards Makers and Their Standards*, Technology Appraisals, 1991.

[TAFIM 1993] *Technical Architecture Framework for Information Management*, Volume 1, *Overview*; Volume 2, *Technical Reference Model (TRM) and Standards Profile Summary;* Volume 4, *Implementation Manual;* Volume 5, *Support Plan;* Volume 6, *DoD Goal Security Architecture (DGSA);* Volume 7, *Information Management Technology Standards Guidance Open Systems Environment (ITSG-OSE)*, November 1993.

[Tang 1992] *Open Networking with OSI*, Adrian Tang and Sophia Scoggins, Prentice Hall, 1992.

[Tater 1989] *Briefing on Secure Data Network Systems (SDNS) to the Protocol Standards Steering Group*, Gary Tater and Greg Bergren, National Security Agency, 25 October 1988, Record of the 35th Meeting of the PSSG, Defense Communications Engineering Center, 6 January 1989.

[Telecoms 1989] "La Galaxie de la Normalisation," *Telecoms Magazine*, 1989.

[Terrell 1990] *Electronic Information Exchange Standards Requirements*, Robert Terrell, Workshop on Electronic Information Exchange Standards Used in Document Processing Applications, NIST, Gaithersburg, MD, 30 July 1990.

[Thacker 1987] "TOP 3.0 Update," Bharat Thacker, *MAP/TOP Interface*, Volume 3, Number 2, MAP/TOP/SME, Spring 1987.

[Thieme 1993] "A Tactical Command Point Network Using IEEE 802.6 MAN Standard," Bernhard P. Thieme, TNO Physics and Electronics Laboratory (The Netherlands), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Thomas 1993] "Heterogeneous Application Interoperability," Anne Thomas, *Open Systems Standards Tracking Report*, Volume 2, Number 3, May 1993, pp. 1-3.

[Thompson 1993a] *Multicast Extensions to Procedure Class 4 of the Protocol for Providing the Connection-mode Transport Service (ISO/IEC 8073:1992)*, K. Thompson, X3S3.3-93-191, April 1993.

[Thompson 1993b] *Description of Multicast Extensions to TP4*, K. Thompson, X3S3.3-93-192, April 1993.

[TRM 1993] *Department of Defense Technical Architecture Framework for Information Management*, Coordination Draft, Version 2.0, 22 June 1993.

[TSGCE 1985] *Corrigendum to the Terms of Reference for the Subgroup on Data Processing and Distribution (SG9)*, AC302-D162(2nd Revise), 24 July 1985, TSGCE, NATO UNCLASSIFIED.

[TSGCE 1988] *NATO Requirements for Open Systems Management*, NATO/AC302 (TSGCE)SG/9MAN.0688/01, AHWG on OSI Management, TSGCE SG/9, 1 July 1988, NATO UNCLASSIFIED.

[TSGCE 1989] *Report of AC/302 (TSGCE) Meeting Held on 10-12 October 1989*, US Mission NATO, 20 October 1989, UNCLASSIFIED.

[TSGCE 1989a] *NATO SG/9 WG/1 18-Month Work Plan*, WG/1, October 1989, NATO UNCLASSIFIED.

[TSGCE 1989b] *Report to SG/9 by the Chairman of WG/1 on the 16th Meeting Held 2-4 October 1989*, 20 October, 1989, NATO UNCLASSIFIED.

[TSGCE 1989c] *Report of AC/302 (TSGCE) Meeting Held on 10-12 October 1989*, US Mission NATO, 20 October 1989, NATO UNCLASSIFIED.

[TSGCE 1989d] Private Communication with the Chair, TSGCE SG9 WG1, 14 March 1989, UNCLASSIFIED.

[TSGCE 1990] *One-Time Meeting on Naming and Addressing*, Secretary for TSGCE SG9, 24 May 1990, NATO UNCLASSIFIED.

[TSGCE 1990b] *Discussions at the US Postcoordination Meeting*, TSGCE SG9, 18-19 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990c] *Chairman's Report on the 10th Meeting Held at NOSC San Diego, USA, 5th to 9th February 1990, AC/302(TSGCE) SG/9 Ad Hoc Working Group on OSI Management*, February 1990, NATO UNCLASSIFIED.

[TSGCE 1990d] *Use of OSI Standards in NATO—Strategic and Technical Issues*, Draft for Issue 3, Contribution by the UK to TSGCE SG9, 4 May 1990, NATO UNCLASSIFIED.

[TSGCE 1990e] *Report to TSGCE by Chairman Subgroup 9*, TSGCE SG9, 5 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990f] *Briefing to TSGCE SG9 on a Proposal for a New TOR for SG9*, Chairman of SG9, May 1990, NATO UNCLASSIFIED.

[TSGCE 1990g] *The TSGCE Subgroup 9 Support Programme for OSI in Military Communications*, Ian White, Admiralty Research Establishment (ARE), UK MOD, Proceedings of the Military OSI Symposium, SP-8, Volume 1 (Unclassified Paper), File Reference 9980, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990h] *The Use of OSI in Military Communications*, Ian White, Admiralty Research Establishment (ARE), UK MOD, Proceedings of the Military OSI Symposium, SP-8, Volume 1 (Unclassified papers), File Reference 9980, SHAPE Technical Centre, 6-8 June 1990, NATO UNCLASSIFIED.

[TSGCE 1990i] *Report of AC/302 SG/9 on WG/2 Activities (Brussels, February 1990)*, WG/2, 14 March 1990, NATO UNCLASSIFIED.

[TSGCE 1990j] *Draft Proposed Terms of Reference for WG3*, WG/3, 22 January 1990, NATO UNCLASSIFIED.

[TSGCE 1990k] *Report of the TSGCE Subgroup 9 on Data Processing and Distribution Meeting Held 9-11 May 1990*, US Representative (O. Schultz), May 1990, NATO UNCLASSIFIED.

[TSGCE 1990l] *Report on the SG/9 AHWG-OSI Management Meeting Held in San Diego During 5-9 February 1990*, US Representative (Lew Gutman), 13 February 1990, UNCLASSIFIED.

[TSGCE 1990m] *Chairman's Report of the 8th Meeting*, AC/302(TSGCE)SG/9 Ad Hoc Working Group on Security, May 1990, NATO UNCLASSIFIED.

[TSGCE 1991] *UK Statement on the Current Status of the Quality of Service Work*, Contribution to TSGCE SG9/WG2, 19 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991a] *Use of OSI Standards in NATO—Strategic and Technical Issues*, Draft, for Issue 4, Contribution by the UK to TSGCE SG9, 8 February 1991, NATO UNCLASSIFIED.

[TSGCE 1991b] *Report of the Chairman of SG9 on the Chairman's meeting of 10 December 1991*, TSGCE SG9, December 1991, NATO UNCLASSIFIED.

[TSGCE 1991c] *US Requirements to Reactivate the Multipeer Data Transmission Project (JTC 1.21.09.01)*, US Contribution to SC21/WG1, 7 March 1991, UNCLASSIFIED.

[TSGCE 1991d] *Comments on Transport STANAGs*, UK Contribution to WG1, United Kingdom, 21 March 1991, NATO UNCLASSIFIED.

[TSGCE 1991e] *WG2 Chairman's Report to SG9*, 4 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991f] *Status Report of the AC/302(SG/9) Ad Hoc Management Group*, 1 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991g] *Multifunction Information Distribution System (MIDS) Low Volume Terminal (LVT) International Cooperative Program*, Briefing of US Representative to PG9 to the US SG9 Coordination Group, 29 October 1991, NATO UNCLASSIFIED.

[TSGCE 1991h] *MMHS AHWG Rationale Document*, Working Draft, 30 September 1991, NATO UNCLASSIFIED.

[TSGCE 1991i] *US/EUROCOM's Role in Developing Profiles for NATO*, AC302/SG9/ WG1-8910/15(NO), 2 October 1989, NATO UNCLASSIFIED.

[TSGCE 1991j] *Phase I Final Report*, TSGCE SG11/PG6 on Tactical Communications Systems for the Land Combat Zone—Post 2000, Submitted to SG11 on 13 November 1991, NATO RESTRICTED.

[TSGCE 1991k] *Report to the Tri-Service Group by the Chairman of the Subgroup on Information Systems*, AC/302(SG/12)D/7, 21 November 1991, NATO UNCLASSIFIED.

[TSGCE 1991m] *Report to the Tri-Service Group by the Chairman of the Subgroup on Information Systems*, AC/302(SG/12)D/7, Appendix 3 to Annex III to AC/302-D/621, AC/302(SG/12)D/7, 21 November 1991, NATO UNCLASSIFIED.

[TSGCE 1991n] *UK Statement on the Current Status of the Quadrilateral Interoperability Programme (QIP) from a National Viewpoint*, Paper Provided to TSGCE SG9/WG2, 19 September 1991, NATO UNCLASSIFIED.

[TSGCE 1991o] *Report of the TSGCE SG9/WG2 Meeting of 30 September to 4 October 1991*, US Representative to WG2 (LCdr Katie Bryant), October 1991, NATO UNCLASSIFIED.

[TSGCE SG12/WG2 1993] *TSGCE Subgroup 12 on Information Systems, Working Group 2 on Data Processing and Management Meeting Held at NATO Headquarters from 8-10 February 1993*, Decision Sheet, AC/302(SG/12-WG/2)DS/6, Martin Krick, Chairman SG12/WG2, 15 March 1993, NATO UNCLASSIFIED.

[TSGCE SG9 1992a] *Army Tactical Command and Control Information System (ATCCIS) Working Paper 25, Technical Standards for CCISs*, Edition 3, DS(CCC-IP)(92)123, AC/302(SG/9), 25 February 1992, NATO UNCLASSIFIED [50 copies made for distribution to TSGCE Subgroup 9, NACISA, NACMA, NAPMA, and interested International Staff at NATO Headquarters].

[TSGCE SG9 1992a] *Procedural Standards for Military Message Handling System (MMHS)*, DS(CCC-ICP(92)370 and AC/302(SG/9), Chairman TSGCE SG9, 3 July 1993, NATO UNCLASSIFIED.

[Turner 1993] "CLNS and CONS Issues for NATO Networking," Geoff Turner, Defence Research Agency-Malvern (United Kingdom), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[UK 1988] *Use of OSI Standards in NATO—Strategic and Technical Issues*, AC/302(SG/9)D/19(Revised), United Kingdom for TSGCE SG9, 1 March 1988, NATO UNCLASSIFIED.

[UK 1990] *NATO as an ISO International Registration Authority, UK Contribution to TSGCE SG9*, May 1990, NATO UNCLASSIFIED.

[Unix 1991] "UI-ATLAS Formally Launched," *Unix International Gazette*, Volume 3, Number 4, November 1991, p. 1.

[Unix 1992] *UNIX International Roadmap for System V and Related Technologies: Executive Summary*, UNIX International, 1992, p. 1.

[US 1988] *Compatibility of STANAG 4214 and GOSIP Network Layer Addressing*, US Input to WG/1, August 1988, NATO UNCLASSIFIED.

[USMCEB 1989] *Directory—US Participants in the International C3 Fora*, US Military Communications Electronics Board, Joint Staff, March 1989, UNCLASSIFIED.

[USPR 1989] *Briefing to TSGCE SG9 WG2 on ACP 127 and CCITT X.400 Service Element Comparison*, US Principal Representative, January 1989.

[Valuer 1993] "System Technology in Tactical Networks," Olaf Valuer and Bjorn Rossow, Alcatel Telecom AS (Norway), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[van der Jagt 1991] "Wiring Media," Larry van der Jagt, *Handbook of Local Area Networks*, John P. Slone and Ann Drinan, Editors, Auerbach Publishers, 1991.

[van der Voort 1990] *Post 2000 Communications Architectures*, A. T. A. M. van de Voort, TNO Physics and Electronics Laboratory, Netherlands, Proceedings of the SHAPE Technical Centre Military OSI Symposium, 6-8 June 1990, NATO UNCLASSIFIED.

[VanEpps 1994] Private Communication from MAJ Roger J. VanEpps, Data Administration Staff Officer, HQ USAF/SCTA, 16 February 1994, UNCLASSIFIED.

[Vernocchi 1992] "PIMB (PCTE Interface Management Board) Association," Luciano Vernocchi, *Open Systems Tracking Report*, Volume 1, Number 4, July 1992, p. 4.

[Vicini 1994] Private Communication with Cristina Vicini, NATO Air Command and Control System Management Agency (NACMA), 27 January 1994, NATO UNCLASSIFIED.

[Wallace 1991] "The JPEG Still Picture Compression Standard," Gregory K. Wallace, *Communications of the ACM*, Volume 34, Number 4, April 1991, pp. 31-44.

[Walmsley 1990] Private Communication with Clive Walmsley, RSRE, UK MOD, 27 March 1990.

[Walsh 1994] Private Communication with Phil Walsh, IDA, 24 February 1994.

[Walters 1992] Private Communication with Dale Walters and Richard Collela, NIST, 8 January 1992.

[Walters 1993] Private Communication with Dale Walters, NIST, 1993.

[Wells 1993] "NATO C3 Architecture LANs and WANs—Internetworking—TP4/CLNP," El J. Wells, USNATEX/NACISA (MITRE USDC3FOI) (Belgium), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Welter 1994] Private Communication with MAJ Richard Welter, SHAPE/Plans and Policy Division, 24 January 1994.

[White 1993] "Principles vs. Pragmatism in Military CIS Interoperability," Ian White, Defence Research Agency-Portsdown (United Kingdom), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Winkler 1991] Private Communication with Jerry Winkler, Chair, ANSI X3H4 on IRDS standards, 18 April 1991.

[Wizgall 1993] "Personal Communication Networks and Services," Manfred Wizgall, Alcatel SEL AG (Germany), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[Wood 1993] "Multicasting Requirements and Standardization Strategies," David C. Wood, MITRE (United States), *Proceedings of the Symposium on Military Communication Networks Interoperability and Standards Held at the SHAPE Technical Centre 8-11 June 1993*, STC Symposium Proceedings SP-10, June 1993, NATO UNCLASSIFIED.

[WP 60 Annex 1990] *Statement of the Requirement for a NATO Data Management Policy, Annex to AC/317 (WG/2) WP/60 on Data Management, Working Paper, Information Systems Working Group*, NACISA, 5 June 1990, NATO UNCLASSIFIED.

[WP7L 1989] *Data Management, Standardization, and Naming Conventions*, ATCCIS Working Paper 7L, Edition 1.0, 2 June 1989, NATO UNCLASSIFIED.

[X.400 1989] Private Communications with Three Members of the NIST X.400 Special Interest Group, 25 May-14 June 1989.

[X/OPEN 1987] *X/OPEN Portability Guide*, Volume 5, *Data Management, X/OPEN Group*, Amsterdam, January 1987.

[X/OPEN 1987a] *X/OPEN Portability Guide*, Volume 1, *System V Specification Commands and Utilities*, X/OPEN Group, Amsterdam, January 1987.

[X/OPEN 1988] *Briefing on X/OPEN, X/OPEN Group*, Amsterdam, 2 March 1988.

[X/Open 1992] *Part 1 of X/Open Systems and Branded Products: XPG4*, X/OPEN Group, Amsterdam, 1992.

[X3 1990] "Standardization Activities," *Computer Standards and Interfaces*, Volume 11, Number 1, 1990, p. 78.

[X3 1991] *X3 Announces the Approval of a New Project on Addenda to ISO 8613*, News Release from Accredited Standards Committee X3, Information Processing Systems, April 4, 1991.

[X3 1991a] *X3 Announces the Second Public Review and Comment Period of X3.190-199x, Conformance Testing for SGML*, Accredited Standards Committee X3, News Release, 16 April 1991.

[X3 1991b] *X3 Announces the Approval of a New Project on Group MAC Addresses to be Published as a Type 3 Technical Report*, Accredited Standards Committee X3, News Release, 9 April 1991.

[X3 1991c] *X3 Announces the Approval of a New Project on Source Routing Transparent (SRT) Bridging for Local Area Networks*, Accredited Standards Committee X3, News Release, 9 April 1991.

[X3 1991d] *X3 Announces the Approval of a New Project on Guidelines for Bridged LAN Source Routing Operation by End System to be Published as a Type 3 Technical Report*, Accredited Standards Committee X3, News Release, 9 April 1991.

[X3 1991e] *X3 Announces a Call for Comments on X3 Project 682-D, Domestic Public/Private X.25 Network Interworking*, Accredited Standards Committee X3, News Release, 5 March 1991.

[X3 1991f] *X3 Announces the Formation of a New Technical Committee, X3T6, Non-Contact Information System Interface*, Accredited Standards Committee X3, News Release, 25 March 1991.

[X3 1991g] *X3 Announces the Approval of a New Project on X.25 Data Transfer Phase Procedures for Operating the Packet Layer Transfer Phase of X.25*, Accredited Standards Committee X3, News Release, 11 March 1991.

[X3 1991h] *X3 Announces the Approval of a New Project for a Numerical C Extension Technical Report*, Accredited Standards Committee X3, News Release, 10 April 1991.

[X3 1991i] *X3 Announces the Approval of a New Project on X Window System Data Stream Definition Part IV: Mapping onto Open Systems Interconnection (OSI) Services*, Accredited Standards Committee X3, News Release, April 23, 1991.

[X3 1991j] *Concerns on Progression of Management Access Control CD*, X3T5/91-390, 26 September 1991.

[X3 1991k] *X3 Announces the Approval of a New Project for Data Compression, Adaptive Coding with Sliding Window for Information Interchange*, Accredited Standards Committee X3, News Release, October 28, 1991.

[X3 1991m] *X3 Announces the Approval of a New Project for Programming Language C Information Bulletins*, Accredited Standards Committee X3, News Release, September 16, 1991.

[X3 1991n] *X3 Announces the Public Review and Comment Period of ISO 11404: Information Technology - Programming Languages - Common Language-Independent Data Types*, Accredited Standards Committee X3, News Release, 3 October 1991.

[X3 1991o] *US Contribution on ISO/IEC CD 10745: Upper Layers Security Model*, Accredited Standards Committee X3T5, 1 October 1991.

[X3 1992] *ASC X3 Announces the Formation of a New Technical Committee, X3H7, Object Information Management (OIM)*, X3 News Release, 3 February 1992.

[X3 1992a] *Response to SC21 N 6232, "Preliminary TP Security Model,"* US National Body, ASC X3T5 92-91, 5 March 1992.

[X3 1992b] *Proposed US Contribution on Definition of Expiry Behaviour*, X3T5/92-149, 6 March 1992.

[X3 1992c] *Proposed US Response to ISO/IEC JTC1/SC21 WG4 N1384*, X3T5/92-147, 4 March 1992.

[X3 1992d] *FDDI Station Management (SMT)*, X3.229-199x, 19 August 1992.

[X3 1992e] *Problems with Certifying FTAM Implementations as Conformant*, X3T5/92-109, March 1992.

[X3 1992f] *X3 Announces the Approval of a New Project for Hypermedia and Multimedia Glossary, Addendum to ANSI X3.172-1990*, Accredited Standards Committee X3, News Release, March 3, 1992.

[X3 1992g] *X3J4 Requests Assistance in the Development of the Revision of ANSI X3.23-1985[R1991], Programming Language COBOL*, Accredited Standards Committee X3, News Release, 11 February 1992.

[X3 1992h] *X3 Announces Formation of a New Technical Committee X3J19*, XBase, 26 August 1992.

[X3 1992i] *X3 Announces the Formation of a New Task Group, X3J4.1, Object-Oriented COBOL*, Accredited Standards Committee X3, News Release, 6 October 1992.

[X3 1992j] *FDDI Standard Nearing Completion*, Accredited Standards Committee X3, Information Processing Systems, News Release, 5 October 1992.

[X3 1992k] *X3 Announces the Public Review and Comment Period of ISO/IEC CD 10967-1, Information Technology - Programming Languages, Their Environments and Systems Software Interfaces - Language Compatible Arithmetic - Part 1: Integer and Floating Point Arithmetic*, Accredited Standards Committee X3, Action Request, 28 October 1992.

[X3T2/93-048 1993] *Request for Review and Comment on Knowledge Interchange Format (KIF) (X3T2/93-041)*, X3T2/93-048, 27 April 1993.

[XPG3 1989] *X/OPEN Portability Guide (XPG3)*, Third Edition, X/Open Group, 1989.

[XTP 1988] *XTP/PE Overview*, Greg Chesson, Silicon Graphics, April 1988.

[XTP 1989] *XTP Protocol Definition, Revision 3.4, Protocol Engines, Inc.*, Santa Barbara, California, 17 July 1989.

[Yeh 1992] *An Overview of SEE Activities*, Raymond T. Yeh, International Software Systems, Inc., NIST ISEE Users Group, 9 November 1992.

[Zelkowitz 1992] *NIST/ECMA Frameworks Reference Model: History and Overview*, Marvin V. Zelkowitz, Computer Systems Laboratory, 9 November 1992.

GLOSSARY

GLOSSARY

3GL	Third Generation Language
4GL	Fourth Generation Language
A	Application profile class requiring COTS
AAIS	ACE ACCIS Implementation Strategy
AAL	ATM Adaptation Layer
AAP	Allied Administrative Publication
ABC	ACE ACCIS BICES Capability
ABCA	Australia, Britain, Canada, and America
ABCS	Army Battle Command System (US)
ABDIS	Abonnee Distribute System
AC	Armament Committee (NATO)
AC2IS	Army Command and Control Information System (US)
ACBA	Allied Command Baltic Approaches
ACC	Access Control Center (US DoD, BLACKER)
ACCIS	Automated Command and Control Information System
ACCS	Air Command and Control System (NATO); Army Command and Control System (US)
ACCSA	Allied Communications and Computer Security Agency (NATO Military Committee)
ACCST	Air Command and Control System Document
ACD	Access Control Domain
ACE	Allied Command Europe
ACIS	Access Control Information System (SDNS); Army CIS Agency (UK MOD)
ACISA	Army CIS Agency
ACISSMO	Army Communications and Information System Standards Management Organization (UK)
ACK	Acknowledgment
ACM	Association for Computing Machinery
ACOE	Army Common Operating Environment (US)
ACP	Allied Communications Publication
ACP 127	Allied Communication Publication 127
ACSE	Association Control Service Element (OSI)
AD	Addendum (ISO); Allied Directive
ADAPSO	Association for Data Processing Service Organizations
ADatP	Allied Data Publication
ADCCP	Advanced Data Communications Control Procedures (ANSI X3.66)
ADGE	Air Defense Ground Environment
ADI	Application-Directory (profile)
ADMD	Administration Management Domain
ADP	Automated (Automatic) Data Processing
ADPG	Air Defence Planning Group
ADREP	Air Defence Representatives (NADC)
ADS	Automated Data System; Architectural Design Study
ADSC	Air Defence Software Committee
ADSIA	Allied Data Systems Interoperability Agency (NACISC)
AE	Application Element; Application Environment (WDTR 10000-3)
AEGIS	Airborne Early Warning Ground Integration Segment (NATO)
AEP	Application Environment Profile
AES	Application Environment Specification (OSF)
AEWWG	Air Electronic Warfare Working Group (NATO)
AFATDS	Advanced Field Artillery Tactical Data System
AFCEA	Armed Forces Communications-Electronics Association
AFCENT	Allied Forces Central Europe
AFNOR	Association Francaise de Normalisation (France) (French Association for Standardization)
AFT	Application-File Transfer (profile)
AGCCS	Army Global Command and Control System (US)
AHG	Ad Hoc Group
AHWG	Ad Hoc Working Group
AHWG-FP	Ad Hoc Working Group on Functional Profiles (TSGCE SG9) (discontinued)
AHWG-ISDN	Ad Hoc Working Group on ISDN (TSGCE SG9)
AHWG-MMHS	Military Message Handling System (TSGCE SG9)
AHWG-OM	Ad Hoc Working Group on OSI Management (TSGCE SG9)
AHWG-SEC	Ad Hoc Working Group on Security (TSGCE SG9)
AI	Artificial Intelligence
AIA	Application Integration Architecture (DEC)
AIAA	American Institute for Aeronautics and Astronautics
AIAC	ACCS Implementation Agency (NACMO)
AIE	Ada Integrated Environment (Air Force)
AIIM	Association for Information and Image Management
AIntP	Allied Intelligence Publication
AIPO	ACCS Implementation Project Office
AIS	Automated Information System
AISG	Ada Implementation Subgroup (ISWG)
AIW	APPI Implementor's Workshop
AJPO	Ada Joint Program Office

ALD Application-Library, Documentation (profile)
ALF Application-Level Facility (ATCCIS)
ALS Ada Language System (Army); Application Layer Structure (OSI)
AM ACE Manual
AMAC Asynchronous Media Access Control (FDDI, FFOL)
AMC Air Mission Control (ACCS)
AMH Automated Message Handling; Application-Message Handling (profile)
AMHS Automated Message Handling System
AMM Application-Manufacturing Messaging (profile)
AMPS Automatic Message Processing System (STAMINA)
ANSA Advanced Network Systems Architecture
AMSSA Assured Mission Support Space Architecture
AMWG Air Space Management Working Group (NATO MNC support)
ANCA Allied Naval Communications Agency (NATO Military Committee)
ANDF Architecture-Neutral Distribution Format
ANS ANSI National Standard (United States)
ANSI American National Standards Institute
AO Accredited Organization (ANSI)
AOM Application-OSI Management (profile)
AOPMS Access to the OPM Service (France)
AOR Area of Responsibility
AOW Asia-Oceania Workshop (Sponsored by POSI)
AP Allied Publication; Application Platform (profile)
APAC ACCS Policy and Planning Advisory Committee
APASS Access to the PAS Service (France)
APDU Application Program Data Unit
API Applications Program(ming) Interface
APIA X.400 Applications Programming Interface Association
APIU Adaptive Programmable Interface Unit
APLI ACSE/Presentation Layer Interface
APP Applications Portability Profile (NIST); Allied Procedures Publication
APPI Applications Peer-to-Peer Interface
APPN Applications Peer-to-Peer Network (IBM)
APSE Ada Programming Support Environment
APTL Accredited POSIX Testing Laboratories (NIST)
AR US Army Regulation
ARC Administrative Radio Conference
ARD Application-Remote Database (Access profile)
ARE Admiralty Research Establishment (UK MOD)
ARFA Allied Radio Frequency Agency (NATO Military Committee)
ARPA Advanced Research Projects Agency (US)
ARPANET Advanced Research Projects Agency Network (United States)
ARRC ACE Rapid Reaction Corps
ARRL American Radio Relay League
ARTYWP Artillery Working Party (MAS Army Board, NATO)
AS Accredited Sponsor (ANSI)
ASAS All-Source Analysis System (US Army)
ASC Accredited Standards Committee (ANSI)
ASCII American National Standard Code for Information Interchange
ASE Application Service Element (OSI)
ASI Application Software Interface
ASIS Ada Semantic Interface Specification
ASM Airspace Management (ACCS)
ASME American Society for Mechanical Engineers
ASN Abstract Syntax Notation (OSI)
ASN.1 Abstract Syntax Notation One
ASO Application Service Object (OSI)
ASSET Advanced System and Software Engineering Enabling Technologies
ASW Anti-Surface Warfare (Navy)
ATACC Advanced Tactical Air Command Central (US DoD)
ATAF Allied Tactical Air Force
ATC Air Traffic Control (ACCS)
ATCA Allied Tactical Communications Agency (NATO Military Committee)
ATCCIS Army Tactical Command and Control Information System
ATCCS Army Tactical Command and Control System (US)
ATIS A Tools Integration Standard; Atherton Tools Integration Standard
ATLR Active Transport Layer Relay
ATM Asynchronous Transfer Mode
ATOC Allied Tactical Operations Centre
ATOMAL Security Category
ATOS Advanced Technical Operations Systems
ATP Allied Tactical Publication; Application-Transaction Processing (profile)
ATS Abstract Test Suite
AUTODIN Automatic Digital Network (US DoD)
AVI Audio Visual Interactive Scriptware (JTC 1)
AVT Application-Virtual Terminal (profile)
AWHQ Alternate War Headquarters
AWIS Army WWMCCS Information System (US)
AWWP Amphibious Warfare Working Party (MAS Navy Board, NATO)

B ISDN B Service (64 kbit/second); application profile class requiring CLTS
BAC Balanced Class of Procedures
BASE Baseband
BCA Basic Connection-Oriented Application
BCS British Computer Society; BICES Central Services
BDM BICES Database Management
BER Basic Encoding Rules (ASN.1)
BETE BICES Evolutionary Test Environment
BFA Battlefield Functional Area

BFACS Battlefield Functional Area Control System (US Army)
BFE BLACKER Front End (US DoD)
BICES Battlefield Information Collection and Exploitation Systems
BIH Bureau International de l' Heure (France)
BISDN Broadband ISDN
BITS Base Information Transfer System (Copernicus, US Navy)
BLD BICES Logical Database
BOD Board of Directors
BOM Bit-Oriented Message
BPACS Battlefield Functional Area Controls Systems
BPS BICES Pilot Study
BRDF Draft British Standard
BROAD Broadband
BS British Standards
BSD Berkeley System Definition (UNIX)
BSFT Byte Stream File Transfer (X/Open)
BSI British Standards Institute (United Kingdom)

C2 Command and Control
C2I Command, Control, and Intelligence
C2RA Command and Control Requirements Analysis
C2RM Command and Control Resources Management (ACCS)
C3 Consultation, Command and Control (NATO); Command, Control, and Communications (US DoD)
C4 Command, Control, Communications, and Computers (US DoD)
C4IFTW Command, Control, Communications, Computers, and Intelligence for the Warrior (US DoD)
CA Canada
CAD Computer-Aided Design
CADDETC CAD-CAM Data Exchange Technical Centre (United Kingdom)
CAE Common Applications Environment (X/Open)
CAI Common Architecture for Imaging (IPI)
CAIS Common APSE Interface Set
CALS Continuous Acquisition and Life Cycle Support (formerly Computer Acquisitions and Logistics Support) (US DoD)
CAM Computer-Aided Manufacturing
CAMP Common ABCS Message Parser (US Army)
CAOC Combat Air Operation Center
CAP Conventional Armaments Plan (NATO)
CAPS Conventional Armaments Planning System (NATO)
CASE Common Application Service Elements (OSI Layer 7); Computer-Aided Software Engineering
CASS Common ABCS Support Software (formerly, Common Application Support Software or Common ACCS Support Software) (US)
CAX Computer Aided Exercises
CBEMA Computer and Business Equipment Manufacturers Association (United States)
CC Common Criteria
CCB Configuration Control Board (QIP)
CCIR Comite Consultatif International de Radio (International Radio Consultative Committee)
CCIS Command and Control Information System; also, Command, Control, and Information System
CCITT Comite Consultatif International de Telegraphique et Telephonique (International Telegraph and Telephone Consultative Committee) see ITU-TS
CITIS Contractor Integrated Technical Information Service (US DoD)
CCR Commitment, Concurrency, and Recovery (OSI Layer 7)
CCS Calculus of Communicating Systems (LOTOS); Command and Control Systems (US Army)
CCSDS Consultative Committee on Space Data Systems
CCTA Central Computer and Telecommunications Agency (UK)
CD Committee Draft (ISO)
CDA Computer Design Activity
CD-ROM Compact Disk Read Only Memory
CDIF CASE Data Interchange Format
CDL Common Data Link (program) (US DoD)
CDS Cell-level Directory Service (OSF DCE)
CEC Commission of the European Communities
CECOM US Army Communications-Electronics Command
CEDD Committee for the Exchange of Digital Data (IHO)
CEN Comite Europeen de Normalisation (European Committee for Standardization)
CENELEC Comite Europeen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardization)
CEPAS Cryptographic Equipment for Packet Switching
CEPT Conference Europeenne des Postes et Telecommunications (European Conference of Postal and Telecommunications Administrations)
CEPT/CAC Commercial Action Committee
CEPT/CCH Harmonization Coordination Committee
CEPT/CLTA Liaison Committee for Transatlantic Telecommunications
CER Confidential Encoding Rules (ASN.1); Canonical Encoding Rules (ASN.1)
CFE Conventional Forces Europe
CG-VDI Computer Graphics Virtual Device Interface
CGA Computer Graphics Association
CGI Computer Graphics Interface (Interfacing)
CGM Computer Graphics Metafile

CGMIF Computer Graphics Metafile Interchange Format
CHILL CCITT High Level Language
CHOD-MOD Chief of Defence
CHS Common Hardware Software
CIA Central Intelligence Agency
CICS Customer Information Control System (IBM)
CIDR Classless Interdomain Routing
CIEG Common Information Exchange Glossary
CIGOS Canadian Interest Group on Open Systems
CIGREF Club Informatique des Grandes Enterprises Francaises (France)
CIM Center for Information Management (DISA); Corporate Information Management (US DoD initiative)
CINC Commander-in-Chief
CINCHAN Allied Commander-in-Chief Channel
CIPSO Common IP Security Option; Commercial Intenet Protocol Security Option
CIS Communications and Information System (NATO); CASE Integration Services (committee); Command, Control, Communications, and Information Systems (UK)
CISPR International Special Committee on Radio Interference
CITIS Contractor Integrated Technical Information Service
CL Connectionless (mode)
CLI Call Level Interface (SQL)
CLID Common Language-Independent Data Types
CLIP Common Language-Independent Procedure Calling Mechanisms
CLIPCM Common Language-Independent Procedure Calling Mechanisms
CLNP Connectionless-mode Network Protocol (OSI)
CLNS Connectionless-mode Network Service (OSI)
CLTP Connectionless-mode Transport Protocol (OSI)
CLTS Connectionless-mode Transport Service (OSI)
CM Configuration Management
CM-IS Connection Management Interface Specification
CMA Configuration Management Authority
CMB Configuration Management Board (STAMINA)
CMC Common Mail Calls (XAPIA)
CMD Color Monitor Device
CMF Common Message Format
CMI Communications Interface Profile (ISO/IEC TR 10000-1)
CMIP Common Management Information Protocol (OSI)
CMIS Common Management Information Service (OSI)
CMIS/P Common Management Information Services and Protocols
CMMS Cryptographic Material Management System (Canada)
CMS Command Management System (US Army); Common Mapping Standard; Communication Management System (Canada)
CMU Carnegie Mellon University
CMW Compartmented Mode Workstation
CN Counter Narcotics
CNAD Conference of National Armaments Directors (North Atlantic Council, NATO)
CNR Combat Net Radio
CNSI Communication System/Network Interoperability
CO Connection Oriented (mode); Change Over (systems management function)
COA Course of Action; Central Operating Authority (NATO)
COCMSF Common OSI Connection Management and Support Functions (IEEE)
CODASYL Conference on Data Systems Languages
COE Common Operating Environment
COEC Council Operations and Exercise Committee (NAC in NATO)
COLDCMWG Character-Oriented Language Development and Configuration Management Working Group (ADSIA)
COLOC Change of Location of Command
Comms Communications
COMPUSEC Computer Security
COMSEC Communications Security
CONOPS Continuity of Operations
CONP Connection-Oriented Network Protocol (OSI)
CONS Connection-Oriented Network Service (OSI)
CONUS Continental United States
CORBA Common Object Request Broker Architecture (OMG)
COS Corporation for Open Systems International
COSAC Canadian Open Systems Application Criteria
COSC Coordinating Operational System Control (ZODIAC, The Netherlands)
COSE Common Open (Operating) Software Environment
COSINE Corporation for Open Systems Interconnection Networking in Europe (COSINE)
COTS Connection-Oriented Transport Service (OSI); Commercial Off-the-Shelf
CP Command Post; Change Proposal
CPCN Command Post Communication Network
CPI-C X/Open Common Programming Interface-Communications
CR Central Region (NATO)
CRC Cyclic Redundancy Check
CRT Cathode Ray Tube
CS Command Sequencer (systems management function); Convergence (sublayer of ATM)
CSA Canadian Standards Association
CSDN Circuit Switched Data Network
CSG Computer Scene Generation
CSL Computer Systems Laboratory (NIST)
CSL CALS SGML Library (US DoD)

CSMA Carrier Sense Multiple Access
CSMA/CD Carrier Sense Multiple Access/Collision Detection
CSMF Conceptual Schema Modelling Facility
CSN Circuit Switched Network
CSNI Communications System/Network Interoperability
CSP Communicating Sequential Processes (LOTOS)
CSPDN Circuit Switched Public Data Network
CSS Combat Service Support; Communications Support System (US Navy)
CSSCS Combat Service Support Control System (US Army)
CSWG Communications Systems Working Group (NACISC, WG1)
CTAPS Contingency Tactical Air Control System (TACS) Automated Planning System (US Air Force)
CTIM CASE Tool Integration Models (ANSI)
CTIS Combat Terrain Information System (US Army)
CTMF Conformance Testing Methodology and Framework
CTS Conformance Testing Services (CEN/CENELEC)
CTS-WAN Conformance Testing Services-Wide Area Network
CUA Common User Access (IBM)
CULR Common Upper Layer Requirement
CVSD Continuously Variable Slope Delta (voice transmission modulation)

D ISDN D Service (16 kbit/second); Document
DA Danish Army; US Department of the Army
DAA Data Authentication Algorithm (FIPS 113)
DAC Discretionary Access Control
DAD Draft Addendum (ISO)
DAF Framework for the Support of Distributed Applications (CCITT); Distributed Applications Framework (OSF)
DAFTG Database Architecture Framework Task Group (ANSI)
DAI Distributed Artificial Intelligence
DAM Draft Amendment (ISO)
DAO Document Architecture Operations
DAP Document Application Profile
DAPWG DFTS Architecture and Procurement Working Group (UK)
DARPA Defense Advanced Research Projects Agency (US DoD)
DB Database
DBE Database Enquiry (EWOS)
DBMS Database Management System
DCA Defense Communications Agency (see DISA)
DCC Data Country Code
DCCP Defence Communications Corporate Plan (Australia)
DCE Data Circuit-Terminating Equipment (CCITT); Distributed Computing Environment (OSF)
DCF Data Communication Function
DCM Distributed Computing Model (Bull)
DCPS Data Communications Protocol Standards (US DoD)
DCS Defense Communications System
DCT Digital Communications Terminal (US DoD)
DCW Digital Chart of the World
DDL Data Definition Language
DDN Defense Data Network (US DoD) (now DISN)
DEA Drug Enforcement Agency (US)
DEC Digital Equipment Corporation
DEFSTAN Defence Standard (UK MOD)
DEOS Danish EUROCOM Communication System
DER Distinguished Encoding Rules (ASN.1) [(replaced by Canonical Encoding Rules (CER)]
DFAD Digital Feature Analysis Data
DFR Document Filing and Retrieval
DFS Distributed File System
DFTS Defence Fixed Telecommunications System (UK)
DGIWG Digital Geographic Information Working Group
DGITS Directorate of Information Technology Systems (UK MOD)
DGSA DoD Goal Security Architecture (formerly *DISSP Goal Security Architecture)*
DIA Defense Intelligence Agency
DIB Directory Information Base
DID Data Item Descriptors
DIGEST Digital Geographic Information Exchange Standard
DII Defense Information Infrastructure (US)
DIN Deutsches Institut fur Normung (Federal Republic of Germany)
DIR Directory
DIS Draft International Standard (ISO); Distributed Interactive Simulation (IEEE 1278)
DISA Defense Information Systems Agency (US DoD, formerly DCA); Data Interchange Standards Association
DISN Defense Information System Network
DISNET Defense Integrated Secure Network (US DoD)
DISP Draft International Standardized Profile
DISSP Defense-Wide Information Systems Security Program
DIT Directory Information Tree
DK Denmark
DLCP Data Link Change Proposal (NATO)
DLPI Data Link Protocol Interface
DLWG Data Link Working Group (ADSIA)
DMA Defense Mapping Agency (US DoD)
DME Distributed Management Environment (OSF)
DMF Data Modelling Facility; Data Management Facility (ATCCIS)

DMI	Desktop Management Interface (DMTF)
DML	Data Manipulation Language
DMRM	Data Management Reference Model (SG12)
DMS	Data Management Subsystem (ACE CCISs); Defense Message System (US DoD)
DMS	Defense Message System (US DoD)
DMTF	Desktop Management Task Force
DNI	Detailed Network Interface (IEEE); Detailed Network Interface
DNS	Domain Name System (US DoD)
DNSIX	DoD IIS Network Security for Information Exchange
DOA	Distributed Office Application
DOAM	Distributed Office Applications Model
Doc	Document
DoD	Department of Defense (United States)
DoD-STD	DoD Standard
DoDCSC	US Department of Defense Computer Security Center
DODIIS	DoD Intelligence Information Systems
DoDISS	DoD Index of Standards and Specifications
DoJ	Department of Justice (US)
DOP	Directory Operational Binding Management Protocol
DORIC	Defence Organization Integrated Communications (Australia)
DoS	Department of State (US)
DOTS	DGSA Overall Transition Strategy
DP	Draft Proposal (ISO)
DPA	Document Printing Application
DPC	Defence Planning Committee (NATO)
DPS	Digital Production System (DMA)
DPSN	Defence Packet Switched Network (UK)
DQDB	Distributed Queue Dual Bus (local area network)
DQSO	Defense Quality Standardization Office
DRA	Defence Research Agency (UK MOD)
DRDA	Distributed Relational Database Architecture (IBM)
DRG	Defense Research Group
DS	Directory Services
DSA	Directory System Agent (OSI)
DSG	Distributed System Gateway
DSNET	Defense Secure Network (US)
DSOM	Distributed System Object Model
DSP	Domain Specific Part; Defense Standardization Program (US); Defense Standardized Profile (US)
DSS	Digital Signature Standard
DSSSL	Document Style Segmentation and Specification Language
DST	Decision Support Tool
DTAM	Document Transfer and Manipulation
DTD	Document Type Definition
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTMP	DCPS Technical Management Panel (US DoD)
DTP	Distributed Transaction Processing
DTR	Draft Technical Report (ISO)
DTSS	Digital Topographic Support System (US Army; see CTIS)
DUA	Directory User Agent (OSI)
DVI	Digital Video Interactive
E-Mail	Electronic Mail
E3	End-to-End Encryption
EA	Evolutionary Acquisition
EAC	Echelons Above Corps
EBC	Evolutionary BICES Capability
EC	European Community
ECB	Echelons at Corps and Below
ECCF	Enhanced Communications Functions and Facilities
ECCM	Electronic Counter-Countermeasures
ECE	Economic Commission of Europe (UN)
ECFF	Enhanced Communications Functions and Facilities
ECITC	European Committee for IT Testing and Certification
ECMA	European Computer Manufacturers Association
ECSA	Exchange Carriers Standards Association, Inc.
ED&C	Error Detection and Correction
EDI	Electronic Data Interchange
EDIFACT	Western European Electronic Data Interchange for Administration, Commerce, and Transportation
EDIM	Electronic Data Interchange Messaging
EEI	External Environment Interfaces
EES	Enhanced EUROCOM Standard
EESP	End-to-End Security Protocol
EFTA	European Free Trading Association
EG	Expert Groups (NIST OSI Implementor's Workshop)
EG-DBE	Expert Group on Database Enquiry
EGDIR	Directory Expert Group (EWOS)
EGTP	Expert Group on Transaction Processing (EWOS)
EIA	Electronic Industries Association
EIA/EPC	Engineering Policy Council
EIFEL	Allied Tactical Operations Centre CCIS (ATOC CCIS, also known as the EIFEL Follow-On)
ELINT	Electronic Intelligence
EMD	Engineering and Manufacturing Development
EMPM	Electronic Manuscript Preparation and Markup
EMUG	European Manufacturing Automation Program (MAP) User Group
EN	European Norm (European Standard) (CEN/CENELEC)
ENSCE	Enemy Situation Correlation Element
ENV	European Norm Vornorm (European Experimental Standard) (CEN/CENELEC)
EPA	Environmental Protection Agency (US Government)

EPHOS European Procurement Handbook for Open Systems (CEC)
EPLRS Enhanced Position Location Reporting System
EPRI Electric Power Research Institute
ERA Entity-Relation-Attribute
ES-IS End System to Intermediate System
ESC Electronic Systems Center (US Air Force)
ESF Eureka Software Factory
ESO External Security Object (ISO)
ESPRIT European Strategic Programme of Research and Development in Information Technology
ESQL Embedded SQL
ESRA Engagement Scheduling and Recording Application
ETG EWOS Technical Guide
ETS European Telecommunications Standard (CEC)
ETSI European Telecommunications Standards Institute
EIUF European ISDN Users Forum
EUROCOM EUROGROUP on Cooperation of Tactical Communications Systems
EUTELSAT European Telecommunications Satellite Organization
EV Event (systems management function)
EVS Event Service (OSF's DME)
EWOS European Workshop for Open Systems
EWSA Exponentially Weighted Stochastic Approximation

F interchange format and representation profile class
FAAD Forward Area Air Defense
FACC Feature Attribute Coding Catalog
FAIS Factory Automation Interconnection System
FAS Forward Area System
FC Facilities Control (ZODIAC, The Netherlands); Federal Criteria (US)
FCG Format-Computer Graphics (profile)
FCS Frame Check Sequence; Fast Connection Setup
FD Formal Description
FDDI Fiber Distributed Data Interface
FDDI-LCF-PMD Fiber Distributed Data Interface - Low Cost Fiber - Physical Layer Medium Dependent
FEICO forms field entry instruction control object
FEPCO forms field entry pilot control object
FDI Format-Directory (Data Definitions profile)
FDT Formal Description Technique
FEC Forward Error Correction
FEDISEE Federation of Integrated Software Engineering Laboratories (NIST)
FFM Forschungsinstitut für Funk und Mathematik (Germany)
FFOL FDDI Follow-On LAN
FFOL-AMAC FFOL - Asynchronous Media Access Control
FFOL-IMAC FFOL - Isochronous Media Access Control
FFOL-PHY FFOL - Physical Layer Protocol
FFOL-PMD FFOL - Physical Medium Dependent
FFOL-SMT FFOL - Station Management
FFOL-SMUX FFOL - Service Multiplexer
FIMS Forms Interface Management System
FIPS Federal Information Processing Standard (United States)
FIRP Federal Internetworking Requirements Panel (US)
FLTSATCOM Fleet Satellite Communications
FM Force Management (ACCS)
FMBS Frame-Mode Bearer Service (ISDN)
FMCT Formal Methods in Conformance Testing
FMS Fixed/Mobile Segment
FNC Federal Networking Council (US)
FOD Format-Open Document (profile)
FOIRL Fiber Optic Inter-Repeater Link
FORMETS Message Text Formatting System (NATO)
FORTRAN Formula Translation (programming language)
FRP90 Frigate Replacement Program for the 1990s (NATO)
FSDWG Functional Segment Development Working Group (ADSIA)
FSG Format-SGML (Interchange profile)
FSK Frequency Shift Keying
FSN Final Sequence Number
FSSG Fire Support Subgroup (JTC3A)
FTAM File Transfer, Access and Management (OSI Layer 7)
FTP File Transfer Protocol (US DoD)
FTR Future (standard)
FUI Flow (Control) Unnumbered Information
FVT Format-Virtual Terminal (Registered Object profile)
FWUF Federal Wireless Users Forum (US)

G-LOTOS Graphical LOTOS (profiles)
GAG-R GOSIP Advisory Group on Registration (US)
GAN Global Area Network
GAP stop-gap (non-strategic standard)
GASS Generic Abstract Services for Security
Gbps gigabits per second
Gbytes Billions (thousand millions) of bytes
GCCS Global Command and Control System (US)
GDMI Generic Definition of Management Information (OSI)
GDMO Guidelines for the Definition of Managed Objects
GFADGE German Air Defense Ground Environment
GEX Group of Experts
GHz Gigahertz
GIF Graphics Interchange Format
GIS Geographic Information System
GK Graphic Shelters (HEROS, Germany)
GKS Graphical Kernel System

GKS-3D Graphical Kernel System for Three Dimensions
GLOBIXS Global Information Exchange Systems
GMI Generic Management Information
GNMP Government Network Management Profile
GOSI Generic Operating System Interface
GOSIP Government Open Systems Interconnection Profile
GOTS Government Off-the-Shelf
GPEF Generic Package of Elementary Functions
GPPF Generic Package of Primitive Functions
GRD GOSIP Register Database
GSM Group Special Mobile (The Netherlands car telephone network)
GSTN General Switched Telephone Network
GTDF Generic Transformed Database Format
GTDI EDI Standard (syntax)
GUI Graphical User Interface
GULS Generic Upper Layer Security

HCI Human-Computer Interface
HD Harmonized Document (CEN/CENELEC)
HD-DOMS HyperDesk Corporation's Distributed Object Management System
HDDI High Definition Digital Interface
HDLC High-Level Data Link Control (OSI Layer 2)
HDTV High Definition Television
HDU Hard Disk Unit
HEROS Heeres-Fuehrungsinformationssystem fur die rechnergestuetzte Operations- fuehrung in Staeben
HF High Frequency
HFS Human Factors Society
HIDS Headquarters Information Distribution System (Canada)
HIS Headquarters Information System
HP Hewlett-Packard
HQ Headquarters
HQADF Headquarters Australian Defence Force
HTU Handheld Terminal Unit
HUI Human Interface
HW Hardware
HYTIME Hypermedia/Time-based Structuring Language

I/F Interface
IAB Internet Architecture Board (US DoD)
IAB/IETF Internet Architecture Board/Internet Engineering Task Force
IACSS International Association for Computer Systems Security
IAeG Inter-Agency edi Working Group
IAL International Access Link (The Netherlands)
IAP Interfaces for Applications Portability (ISO/IEC JTC1)
IARRCIS Interim ACE Rapid Reaction Corps Information System (UK, ACE)
IBM International Business Machines
IBN Institut Belge de Normalisation (Belgium)
ICA Integrated Communications Architecture
ICAM Integrated Computer-Aided Manufacturing
ICASE Integrated Computer-Aided Software Engineering (See ISEE)
ICCCM Inter-Client Communications Conventions Manual
ICD International Code Designator
ICL International Computers Limited
ICP Infrastructure Capability Packages
ICS Implementation Conformance Statement
ICSI International Coding System Identifier
ICT Intercept Recommendation (TSGCE SG9)
ID Identification
IDA Institute for Defense Analyses
IDAPI Independent Database API (Borland International, IBM, and Novell)
IDB Integrated Data Base (MIIDS)
IDBEF Integrated Database Extract Format
IDBTF Integrated Database Transaction Format
IDC International Data Corporation
IDEF Integrated Computer-Aided Manufacturing (ICAM) Definition (Language)
IDEF0 IDEF Activity Modeling (Language)
IDEF1X IDEF Data Modeling (Language) Extended
IDI Initial Domain Identifier
IDL Interface Definition Language
IDMR Inter-Domain Multicast Routing (Internet)
IDN Interface Definition Notation (ECMA 127)
IDP Initial Domain Part
IDR Information Distribution and Receipt
IDRP Inter-Domain Routing Protocol
IEC International Electrotechnical Commission
IEE Institution of Electrical Engineers (United Kingdom)
IEEE Institute of Electrical and Electronics Engineers (United States)
IEG Information Exchange Group (NATO)
IEPG Independent European Programme Group (NATO)
IER Information Exchange Requirement
IETF Internet Engineering Task Force
IETM Interactive Electronic Technical Manual (US DoD)
IEW Intelligence and Electronic Warfare
IFF Interchange File Format
IFIP International Federation for Information Processing
IFRB International Frequency Registration Board (UIT)
IFSAS Interim Fire Support Automation System (US Army)
IFU Interworking Functional Unit
IGES Initial Graphics Exchange Specification
IGOSS Industry/Government Open System Specification
IHO International Hydrographic Organization
IIC International Institute of Communications
IIF Image Interchange Facility

IIRS Institute for Industrial Research and Standards (Ireland)
IIS IntelligenceInformation System
IIW ISDN Implementor's Workshop
IJMS Interim JTIDS Message Specification
IKBS Integrated Knowledge-Based System
ILS Integrated Logistics Support
IMA Information Mission Area
IMAC Isochronous Media Access Control (FDDI, FFOL)
IMETS Integrated Meteorological System (US Army)
IMIL Library
IMS International Military Staff (NATO HQ)
IMSC Imagery Standards Management Committee (US DoD)
INFOSEC Information Security
INSTAC Information Technology Standardization Technology Committee
INTAP Interoperability Technology Association for Information Processing (Japan)
INTELSAT International Telecommunications Satellite Organization
INTEROP International Operations
INTSUM Intelligence Summary
INTUG International Telecommunications Users Group
INTWP Intelligence Interservice Working Party (MAS Army Board, NATO)
INX Information Exchange
IOC Initial Operational Capability
IOF Input-Output Facility (ATCCIS)
IONL Internal Organization of the Network Layer
IOT&E Initial Operational Test and Evaluation
IP Internet Protocol; Interoperability Parameter; Internetwork Protocol
IPI Image Processing and Interchange
IPM Interpersonal Messaging (MHS Service)
IPMS Interpersonal Messaging Service (MHS)
IP:ng Next Generation Internet Protocol
IPO IGES/PDES Organization (NIST)
IPSEC Internet Protocol Security Protocol
IPX Internet Packet Exchange
IR International Registry
IRD Information Resource Dictionary
IRDS Information Resource Dictionary System
IRIWP Imagery Reconnaissance and Interpretation Working Party (MAS Air Board, NATO)
IS International Standard (ISO); Intermediate System (OSI); International Staff (NATO HQ)
IS-IS Intermediate System to Intermediate System Routing Protocol
ISA Integrated Systems Architecture
ISAM Indexed Sequential Access Method
ISCS Integrated Satellite Control Services
ISDN Integrated Services Digital Network
ISDN-BW ISDN for the German Armed Forces
ISDN/NUF ISDN Network Users Forum
ISEE Integrated Software Engineering Environment (ISEE) Working Group (NIST)
ISI Information Storage Interface Profile
ISME International Subject Matter Expert
ISO International Organization for Standardization; International Standard
ISO-DCC International Organization for Standardization; International Standard-Data Country Code
ISO-SWG International Organization for Standardization; International Standard-Special Working Group
ISOC Internet Society
ISODE ISO Development Environment
ISP International Standardized Profile
ISPABX Integrated Services Public Access Branch Exchange
IST International Standards
ISUP ISDN Signalling System No. 7 User Part
ISWG Information Systems Working Group (NACISC WG2)
IT Italy; Information Technology
ITD Interim Terrain Data
ITDN Integrated Tactical-Strategic Digital Network (US DoD)
ITF Information Transfer Format
ITI Industrial Technology Institute
ITPB Information Technology Policy Board
ITRC Information Technology Requirements Council
ITS Integrated Tool Set (COS)
ITSB Information Technology Standards Board (UK MOD)
ITSDN Integrated Tactical Strategic Digital Network (US DoD)
ITSEC Information Technology Security Evaluation Criteria
ITSG-OSE Information Technology Standards Guidance for an Open System Environment (TAFIM, US DoD)
ITSTC Information Technology Steering Technical Committee (UK)
ITU International Telecommunications Union
ITU-TS International Telecommunication Union - Telecommunication Standardization Sector (formerly CCITT)
ITU-TSB International Telecommunications Union - Telecommunications Bureau (formerly CCITT)
IUKADGE Improved United Kingdom Air Defence Ground Environment
IUT Implementation under Test
IUW ISDN User's Workshop
IVD Integrated Voice and Data (local area network)
IWF Interworking Function
IWG Information Working Group
IWU Interworking Unit (OSI for relay functional profiles)

J6J US Joint Staff
JANAP Joint Army, Navy, Air Force Publication
JASMIN Joint Analysis System Military Intelligence (Germany national intelligence system)
JBIG Joint Bi-Level Imaging Group
JCS Joint Chiefs of Staff
JINTACCS Joint Interoperability of Tactical Command and Control Systems (US DoD)
JIEO Joint Interoperability and Engineering Organization
JIS Japanese Industrial Standard
JISC Japanese Industrial Standards Committee
JITC Joint Interoperability Test Center (US DoD)
JMCIS Joint Maritime Command and Information System (US Navy, USPACOM)
JMSWG Joint Messaged Standards Working Group (JTC3A)
JOPES Joint Operations Planning and Execution System
JPEG Joint Photographic Experts Group
JROC Joint Requirements Oversight Council (US DoD)
JSA Japanese Standards Association
JTAP JTC1 TAG Applications Portability Study Group
JTC Joint Technical Committee
JTC1 Joint Technical Committee One (ISO/IEC)
JTC3A Joint Tactical Command, Control and Communications Agency
JTF Joint Task Force
JTIDS Joint Tactical Information Distribution System
JTM Job Transfer and Manipulation (OSI Layer 7)
JTSSG Joint Technical Standards Steering Group (DoD)

KAPSE Kernel Ada Programming Support Environment
KBS Knowledge-Based System
kbytes Thousands of bytes
KDC Key Distribution Center (BLACKER)
KDP Key Distribution Protocol
kHz Kilohertz
KIF Knowledge Interchange Format
KIT KAPSE Interface Team
KITIA KAPSE Interface Team from Industry and Academia
KMAE Key Management Application Entity
KMAP Key Management Application Process
KMASE Key Management Application Service Element
KZU Special Signalling Converters (Germany)

LAAD Low-Altitude Air Defense
LACS Local Area Communications Subsystem (The Netherlands)
LAN Local Area Network
LAP B Link Access Procedure, Balanced
LAP D Link Access Procedure, Version D (used for ISDN)
LAS Local Area (Access) Subsystem
lb Pounds
LCAS Language Compatible Arithmetic Standard
LCF Low-Cost Fiber (FDDI)
LCC Limited Capability Configuration
LDM Logical Data Model
LDN Local Distribution Network (Canada)
LEWWG Land Electronic Warfare Working Group (NATO)
LIS Language Independent Specification (IEEE POSIX)
LISA Link in Support of ACCS
LLC Logical Link Control (OSI Network Layer)
LMS License Management Service (OSF's DME)
LMX Local Area Network Manager
LOC Levels of Operational Capability (ACCS)
LOCE Linked Operations-Intelligence Centers Europe; Limited Operational Capability-Europe (US national intelligence system)
LOD Levels of Detail
LOTOS Language of Temporal Ordering of Specification
LPI Low Probability of Intercept
LRC Logistic Reporting Conference (NATO MNC support for ACE)
LRCS Long-Range Communications System (Canada)
LRM Language Reference Model
LTACFIRE Lightweight Tactical Fire Direction System
Ltd Limited
LTDP Long-Term Defence Plan(ning)
LVT Low Volume Terminal
LWER Lightweight Encoding Rules

MAC Media Access Control
MACF Multiple Association Control Function
MACH OSF/1 Microkernel Operating System
MAGTF Marine Air-Ground Task Force (US Marine Corps)
MAN Metropolitan Area Network
MAP Manufacturing Automation Protocol
MAPI Messaging API (Microsoft)
MAPLE Manufacturing Automation Programming Language Environment Architecture
MAPSE Minimum Ada Programming Support Environment
MARREP Maritime Reporting System (NATO)
MAS Military Agency for Standardization (NATO Military Committee)
MBER Minimum Basic Encoding Rules (ASN.1)
Mbps Megabits per second
Mbytes Millions of bytes
MC Military Committee (NATO); Military Characteristic (NATO requirement)
MC&G Mapping, Charting, and Geodesy (DMA)

MCCR	Mission Critical Computer Resources (US DoD)
MCFSS	Marine Corps Fire Support System (US)
MCG	Mapping, Charting, and Geodesy
MCGT	Mapping, Charting and Geodesy Technology Standardization Area (US DoD)
MCS	Maneuver Control System (US Army)
MF	Mediation Function
MFS	Message Formatting System (UK)
MG	Multinational Group (NATO)
Mgd	Managed
Mgmt	Management
MH	Messager Handler
MHEG	Multimedia and Hypermedia Information Coding Experts Group
MHS	Message Handling System (OSI Layer 7); Message Handling Service (Novell, Inc.)
MHz	Megahertz
MIA	Multivendor Integration Architecture
MIB	Management Information Base
MIDLA	Media-Independent Data Link Architecture (TSGCE)
MIDS	Multifunctional Information Distribution System (NATO)
MIF	Management Information File
MIIDS	Military Intelligence Integrated Data System (US)
MIL-STD	Military Standard (US DoD)
MILNET	Military Network (United States)
MIM	(Network) Management Information Model (US DoD)
MIME	Multimedia Internet Mail Extension
MIPS	Management Information Protocol Specification (see CMIP)
MIR	Management Information Register
MIS	Management Information Service (OSI); Management Information System
MISD	Management Information Service Definition (see CMIS)
MIT	Massachusetts Institute of Technology
MITI	Ministry of International Trade and Industry (Japan)
MLP	Multi-Link Procedure (HDLC)
MLS	Multi-Level Secure
MM	Mixed Mode (of Operations in DTAM)
MMHS	Military Message Handling System
MMI	Man-Machine Interface
MML	Man-Machine Language (CCITT Z.300 Series)
MMS	Manufacturing Message Specification (MAP)
MNC	Major NATO Command[er]
MND	Military Need Document (NATO)
MO:DCA	Mixed Object Document Content Architecture
MOA	Memorandum of Agreement
MOCS	Managed Object Conformance Statement
MOD	Ministry of Defence (United Kingdom)
MODITSB	Ministry of Defence Information Technology Standards Board (UK)
MOM	Message-Oriented Middleware Consortium
MOR	Military Operational Requirement (NATO)
mOSI	Minimal Open Systems Interconnection
MOT	Means of Testing
MOTIS	Message-Oriented Text Interchange System (OSI Layer 7)
MOU	Memorandum of Understanding
MPC	Multi-Party Communications
MPD	Multipeer Data
MPDT	Multipeer Data Transmission (OSI)
MPEG	Moving Picture Expert Group
MPMC	Multipeer/Multicast (MPDT)
MPTM	Multi-party Test Methods
MROC	Multicommand Required Operational Capability
MRR	Multi-Role Radio
MS	Message Store (MHS); Mobile Subsystem; Microsoft
MSC	Major Subordinate Command[er] (NATO)
MS-DOS	Microsoft Disk Operating System
MSDSG	Multi-System Distributed System Gateway
MSE	Mobile Subscriber Element (US Army)
MSF	Man-Machine Support Facility
MSMV	Multiple Sampling and Majority Voting
MSP	Message Security Protocol (SDNS)
MT	Message Transfer; Message Terminal (ZODIAC, The Netherlands)
MTA	Message Transfer Agent (MHS)
MTACCS	Marine Tactical Command and Control System
MTF	Message Text Format
MTP	Message Transfer Part (MHS)
MTS	Message Transfer System (The Netherlands); Marine Tactical Systems (US DoD)
MTWP	Maritime Tactical Working Party (MAS Navy Board, NATO)
MUS	Mobile User Subsystem
MWWP	Mine Warfare Working Party (MAS Navy Board, NATO)
N	Notice (ISO Working Paper)
NA	North American
NAAG	NATO Army Armaments Group (CNAD)
NAC	North Atlantic Council (NATO)
NACISA	NATO Communications and Information Systems Agency (NACISC)
NACISC	NATO Communications and Information Systems Committee
NACISO	NATO Communications and Information Systems Organization
NACMA	NATO ACCS Management Agency
NACMO	NATO ACCS Management Organization
NACSI	NATO Advisory Committee for Special Intelligence (NATO Military Committee)
NADC	NATO Air Defence Committee
NADDO	NATO Design and Development Objective
NAEGIS	NATO AEW Ground Integration Segment
NAEW	NATO Airborne Early Warning

NAEW&C NATO Airborne Early Warning and Control
NAFAG NATGO Air Force Armaments Group (CNAD)
NAFIN Netherlands Armed Forces Integrated Network
NAPI North American PCTE Initiative
NAPMA NATO Airborne Early Warning and Control Program Management Agency
NAPO NATO Production Objective
NAS Network Application Support (DEC)
NATO North Atlantic Treaty Organization
NATO-ICD NATO-International Code Designator
NBS US National Bureau of Standards (now NIST)
NBSIR NBS Interim Report
NC NATO Confidential
NCC National Computing Centre
NCCIS NATO Command, Control and Information System
NCD National Contribution Database (BICES)
NCGR Next Generation Computer Resources (Navy)
NCIS NATO Common Interoperability Standards
NCISI Non-Contact Information Systems Interface
NCN NATO Core Network
NCS National Communications System (US DoD); Network Computing Services
NCSC National Computer Security Center
NCSL National Computer Systems Laboratory (NIST)
NCV Support for Naming Convention Validation (IRDS)
NDDN Norwegian Defence Digital Network
NDE News Development Environment (Sun Microsystems)
NDI Nondevelopmental Item
NDL Network Database Language (OSI)
NE The Netherlands
NEC Northern European Command
NEDBAG NATO Emitter Data Base Advisory Group
NEF Network Element Function
NET Telecommunications European Norm
NetBIOS Network Basic Input Output System
NEWAC NATO Electronic Warfare Advisory Committee (NATO Military Committee)
NEWWG NATO Electronic Warfare Working Group
NFR90 NATO Frigate Replacement for the 1990s
NFS Network File System (Sun Microsystems)
NIAG NATO Industrial Advisory Group (CNAD)
NIAM Nijssen Information Analysis Method
NICS NATO Integrated Communications System
NIDL Network Interface Definition Language
NIDTS NATO Initial Data Transfer Service (Program)
NII National Information Infrastructure (US)
NIIF Network Independent Interface (NIAG SG6)
NIIS NATO Interconnected Information System
NIIT National Information Infrastructure Testbed (US)
NILE NATO Improved Link Eleven
NILS Network Internal Layer Structure
NIMP NATO Interoperability Management Plan
NIPD NATO Interoperability Planning Document
NIS NATO Identification System
NISO National Information Standards Organization
NIST US National Institute of Standards and Technology
NITF National Imagery Transmission Format
NITFS National Imagery Transmission Format Standard (US DoD)
NIU North American (NA) ISDN User's (Forum)
NL The Netherlands
NLCP Network Layer Control Protocol (OSI)
NLI Network Layer Interface
NLR Network Layer Relay
NLS Native Language Support (X/Open)
NLSP Network Layer Security Protocol
NM Network Management
NMForum Network Management Forum
NMOS NATO Maritime Operational Intelligence Support
NMA NATO Military Authority
NMP Network Management Profile
NMSIG Network Management Special Interest Group (NAOIW)
NNAG NATO Naval Armaments Group (CNAD)
NNI Nederlands Normalisatie-Instituut (Netherlands)
NNTP Network News Transfer Protocol
NO Norway
NOAA National Oceanographic and Atmospheric Administration (US)
NOIS NATO Operational Interoperability Standards
NORAD North American Air Defense
NOSA NATO OSI Security Architecture
NOSIP NATO Open Systems Interconnection Profile
NOTS NATO Off-the-Shelf
NP New Project (ISO, formerly New Work Item)
NPDU Network Protocol Data Unit
NPI Network Protocol Interface
NPICS NATO Protocol Implementation Conformance Statement
NPIS NATO Procedural Interoperability Standards
NPS Nuclear Planning System
NPT National PDES Testbed (NIST)
NR NATO RESTRICTED
NRZ Non-Return to Zero
NS NATO SECRET
NSA National Security Agency (United States)
NSAI National Standards Authority of Ireland
NSAP Network Service Access Point (OSI)
NSF Network File System
NSG NATO Standardization Group (NAC in NATO)
NSP NATO Standardized Profile
NSS National Standards System (Canada)
NSSN National Standards System Network (US, developed by NIST)

NST	NATO Staff Target
NT	New Technology
NTF	National Transfer Format (United Kingdom)
NTIS	NATO Technical Interoperability Standards; National Technical Information Service (United States)
NTP	Network Time Protocol
NTSC	National Television System Committee
NTT	Nippon Telegraph and Telephone Corporation (Japan)
NU	NATO UNCLASSIFIED
NUICS	North American Air Defense (NORAD) USPACECOM Integrated Command and Control System
NVLAP	National Voluntary Laboratory Accreditation Program (NIST)
NWI	New Work Item (ISO) (see also NP)
O/R	Originator/Recipient (MHS)
O&M	Operations and Maintenance
OC	Optical Carrier (SONET level)
OCONUS	Outside the Continental United States
ODA	Office Document Architecture
ODAC	Office Document Architecture Consortium
ODBC	Open Database Connectivity (Microsoft)
ODIF	Office Document Interchange Format
ODL	Office Document Language
ODP	Open Distributed Processing
OIM	Object Information Management
OIW	OSE Implementor's Workshop
OM	OSI Management
OMA	Object Management Architecture (OMG)
OMB	Office of Management and Budget (US)
OMG	Object Management Group
OMIPoint	Open Management Interoperability Point
ONC	Open Network Computing (Sun Microsystems)
OODBTG	Object-Oriented Database Task Group (ASC X3)
OpenISE	Open Information Systems Engineering (CEC)
OPM	Operational Messaging (France)
OPWP	Operational Procedures Working Party (MAS Army Board, NATO)
ORB	Object Request Broker (OMG)
ORBAT	Order of Battle
OS	Operating System
OS/2	Operating System 2 (IBM)
OSA	Open System Architecture (Olivetti)
OSC	Operational System Control (ZODIAC, The Netherlands)
OSCRL	Operating System Command and Response Language
OSD	Office of the Secretary of Defense (US DoD)
OSE	Open System Environment
OSF	Open Software Foundation
OSI	Open Systems Interconnection
OSI/NMF	Open Systems Interconnection/Network Management Forum
OSIE	Open Systems Interconnection Environment
OSINET	Open Systems Interconnection Network
OSINLCP	OSI Network Layer Control Protocol
OSIP	Open Systm Interoperability Profile
OSITOP	Open Systems Interconnection for Technical and Office Protocol
OSITP	OSI Transaction Processing
OSN	Open Systems Newsletter
OSSAI	Open Systems Standard Applications Interface
OSTC	Open Systems Testing Consortium
OSTF	Object Services Task Force (OMG)
OTF	Open Token Foundation
P1	Message Transfer Protocol (MHS)
P2	Interpersonal Messaging Protocol (MHS)
P3	MTS Access Protocol (MHS)
P7	Message Store Access Protocol (MHS)
PA	Identifier of the Profile Class for AEPs
PABX	Public Access Branch Exchange
PAD	Packet Assembly/Disassembly
PADP	Panel on Air Defence Philosophy (NADC)
PADW	Panel on Air Defence Weapons (NADC)
PAL	Phase Alternating Line
PAPS	Phased Armaments Programming System (NATO)
PAR	Project Authorization Request (IEEE)
PAS	Publicly Available Specification; data-only transmission protocol (France)
PASC	Portable Application Standards Committee (IEEE) [(formerly Technical Committee on Operating System (TCOS)]
PBX	Private Branch Exchange
PC	Personal Computer
PCIS	Portable Common Interface Set
PCM	Pulse Code Modulation; Procedure Call Mechanism
PCNCEP	Political Consultation and NATO Civil Emergency Planning
PCO	Point of Control and Observation
PCS	PC Services (OSF's DME)
PCT	Personal Computer Teletype (ZODIAC, The Netherlands)
PCTE	Portable Common Tool Environment
PCTS	POSIX Conformance Test Suite
PCU	Portable Computer Unit (US Army); Programmable Control Unit (packet radio)
PDAD	Proposed Draft Addendum (ISO)
PDAM	Proposed Draft Amendment (ISO)
PDES	Product Definition Exchange Specification
PDIF	Product Definition Interchange Format
pDISP	Proposed Draft International Standardized Profile
PDL	Page Description Language; Program Design Language
PDN	Public Data Network
PDTR	Proposed Draft Technical Report

PDU	Protocol Data Unit
PEB	Planning and Execution Board (QIP)
PEI	Platform External Interface (TR 10000-3)
PEICO	Paged Field Entry Instruction Control Object
PEPCO	Paged Field Entry Pilot Control Object
PEM	Privacy Enhanced Mail
PEO-CCS	Program Executive Officer, Command and Control Systems (US Army)
PER	Packed Encoding Rules (ASN.1)
PEX	PHIGS Extension to X
PG	Project Group
PHIGS	Programmer's Hierarchical Interactive Graphics System
PHQs	Peace Headquarters
PHY	Physical
PI	Identifier of the Profile Class for Interface Profiles
PICS	Protocol Implementation Conformance Statement
PII	Protocol Independent Interface (IEEE)
PIK	Programmer's Imaging Kernel
PIKS	Programmer's Imaging Kernel System
PIMB	PCTE Interface Management Board
PIWG	Permanent Interoperability Working Group (ADSIA)
PLI	Position Location Information; Presentation Library Interface (UI)
PLP	Packet Level Protocol (X.25)
PLPS	Presentation Level Protocol Syntax
PM	Processable Mode (of Operations in DTAM)
PMD	Physical Layer Medium Dependent
PMS	Packet Multicast Service
PN	Project Number
PNL	Pacific Northwest Laboratories
POC	Profile for Open System Environment Components (EWOS)
POCAC	APIs for Communications Services (EWOS OSE Profiles)
POCAI	APIs for Information Services (EWOS OSE Profiles)
POCAS	APIs for System Services (EWOS OSE Profiles)
POCAU	APIs for End-User Services (EWOS OSE Profiles)
POCF	Formats (EWOS OSE Profiles)
POCL	Look and Feel Definitions (EWOS OSE Profiles)
POCP	Protocols (EWOS OSE Profiles)
PODA	Piloting Open Document Architecture
POE	Profiles for Open System Environment (EWOS)
POSC	Petrochemical Open Software Corporation
POSI	Promoting Conference for OSI (Asia-Oceania Regional Workshop)
POSIX	Portable Operating System Interface for Computer Environments
PPP	Point-to-Point Protocol
PPRDB	Partitioned, Partially Replicated Database
PPSC-IT	Public Procurement Subcommittee in the Information Technology Sector (CEC)
PPTM	Protocol Profile Conformance Testing Methodology
prENV	Draft European Pre-Standard
PREMO	Presentation Environment for Multi-Media Objects
PRL	Profile Requirements List
PRMD	Private Management Domain
PROST	Program of Research on Open System Testing
PRS	Print Management Service (OSF's DME)
PSC	Principal Systems Command; Principal Subordinate Command[er]; Primary Subordinate Command
PSDN	Packet Switched Digital Network
PSEIF	Project Support Environment Interfaces Standard (Navy)
PSESWG	Project Support Environment Standards Working Group (Navy)
PSN	Packet Switched Network
PSPDN	Packet Switched Public Data Network
PSPvtDN	Packet Switched Private Data Network
PSSG	Protocol Standards Steering Group
PSTN	Public Switched Telephone Network
PSTP	Protocol Standards Technical Panel (see DTMP)
PTI	Public Tool Interface
PTLR	Passive Transport Layer Relay
PTS	Profile Test Specification
PTT	Postal, Telegraph, and Telephone
PVC	Permanent Virtual Circuit
PWG	Permanent Working Group (ATCCIS)
PWI	Public Window Interface (specification)
Q&A	Question and Answer (NATO Identification System)
QCMP	Quadrilateral Configuration Management Plan
QIFS	Quadrilateral Interoperability Field System (UK)
QIP	Quadrilateral Interoperability Programme
QIPMP	Quadrilateral Interoperability Programme Management Plan
QMHS	Quadrilateral Message Handling System
QoS	Quality of Service
QP	Quadrilateral Profile
QRMP	Quick-Reaction Multicolor Printer (US Army)
QSTAG	Quadrilateral Standardization Agreement
QTDMP	Quadrilateral Test and Demonstration Management Plan
QTIDP	Quadrilateral Technical Interface Design Plan
QTIR	Quadrilateral Technical Interface Requirement
QWERTY	Arrangement of keys on US standard keyboard
R	Relay (profile class)
R&R	Review and Release
RA	Remote Actions (FTAM)

RACWG Requirement and Design Criteria Working Group (CAIS)
RADIUS Research and Development for Image Understanding Systems (US ARPA)
RAM Random Access Memory
RAP Recognized Air Picture (ACCS); Radio Access Point
RARE Reseaux Associes pour le Recherche Europeenne (Association of European Research Networks)
RD Restricted Data
RDA Remote Data Access (OSI)
RDBMS Relational Database Management System
RDCE RADIUS Common Development Environment (US ARPA)
RDN Relative Distinguished Name
RDT Referenced Data Transfer
Re/KK Computer Communication Shelters (Germany)
RFC Request for Comment
RFP Request for Proposal
RFT Request for Technology
RGB Red-Green-Blue
RGPF Raster/Gridded Product Format
RIPSO Revised Internet Protocol Security Option
RL Requirements List
RLE Run Length Encoding
RM Reference Model; Relationship Management (systems management function)
RMDM Reference Model on Data Management
RNLA Royal Netherlands Army
RO Remote Operations
RODE Remote Open Document Editing
ROMC Required Operational Messaging Characteristic
ROS Remote Operation Service (OSI)
ROSE Remote Operation Service Element (OSI)
RPC Remote Call Procedure
RSP Recognized Sea Picture
RSRE Royal Signals and Radar Establishment
RSTA Reconnaissance, Surveillance, and Target Acquisition
RT Reliable Transfer
RTA Reliable Transfer Agent
RTDSC Real-Time Distributed Systems Communication (POSIX)
RTM Response Time Monitoring (systems management function)
RTS Reliable Transfer Service (OSI)
RTSE Reliable Transfer Service Element (OSI)
RTTS Real-Time Transport Service
RWCC Regional Workshop Coordinating Committee
RWS-CC Regional Workshop Coordinating Committee

SA Security Association; Structured Analysis
SA-P Security Association (SA) - Protocol
SAA Systems Application Architecture (IBM)
SABM Set Asynchronous Balanced Mode
SACEUR Supreme Allied Commander Europe
SACF Single Association Control Function
SACLANT Supreme Allied Commander Atlantic
SAG SQL Access Group
SAIF Spatial Archive and Interchange Format
SAM Surface-to-Air Missile
SAME SQL Ada Module Extensions
SAMeDL SQL-Ada Module Description Language
SAMOC Surface-to-Air Missile Operations Center
SANISI Security Architecture for NATO Information Systems Interconnection
SANTIS Single Architecture of NATO Technical Common Interface Standards
SAO Single Association Object
SAP Service Access Point; Subnetwork Access Protocol (Network Layer)
SAPI Service Access Point Identifier (LAPD)
SAR Segmentation and Reassembly
SARWP Search and Rescue Working Party (MAS Air Board, NATO)
SASO Saudi Arabian Standards Organization
SATCOM Satellite Communications
SC Sub-Committee (ISO); Study Committee
SCARS Status Control Alerting and Reporting System
SCC Standards Council of Canada
SCCOA Systeme de Controle et de Commandement des Operations Aeriennes (France)
SCCS Source Code Control System (AT&T)
SCECP Senior Civil Emergency Planning Committee (NAC in NATO)
SCF Service Control Facility (ATCCIS)
SCI Sensitive Compartmented Information
SCPS-TWG Space Communications Protocol Standards Technical Working Group (US)
SCRA Single-Channel Radio Access
SCSI Small Computer System Interface
SCWUI Steering Committee on User Interface (IEEE)
SD Structured Design
SD&IC System Design and Integration Contract (ACE ACCIS)
SDCP Subnetwork Dependent Convergence Protocol (OSI Network Layer)
SDE Secure Data Exchange (IEEE); System Development Environment
SDH Synchronous Data Hierarchy
SDIF SGML Document Interchange Format
SDIO Strategic Defense Initiative Office
SDL System Development Language (FDT)
SDLC Synchronous Data Link Control
SDN Secure Data Network
SDNS Secure Data Network System (US National Security Agency)
SDS Software Distribution Service (OSF's DME); Strategic Defense System (US DoD)
SDTS Spatial Data Transfer Specification
SDU Standalone Display Unit
SE Service Element

SECAN Military Committee Communications Security and Evaluation Agency (NATO)
SEE Software Engineering Environment
SEI Security Exchange Information
SEP System Execution and Planning (ZODIAC, The Netherlands)
SESE Security Exchange Service Element
Seq Sequence
SFA Specified Subfunctional Area; Sensor Fusion Area (ACCS)
SFS Suomen Standardisoimisliitto (Finland)
SG Subgroup
SGFS Special Group on Functional Standardization (ISO/IEC JTC1)
SGML Standard Generalized Markup Language
SHAPE Supreme Headquarters Allied Powers Europe
SHF Super High Frequency
SHIF SHAPE Information Flow
SHORAD Short-Range Air Defense
SIB Systems Interoperability Branch (CIS Division, IMS, NATO)
SICF Systeme Informatique de Commandement des Forces Terrestres
SICP Subnetwork Independent Convergence Protocol (OSI Network Layer)
SIF SSDB Interchange Format
SIG Special Interest Group (NIST OSI Implementor's Workshop)
SIGMA UNIX Open Applications Group
SIGCOMM Special Interest Group on Data Communications (ACM)
SIGINT Signals Intelligence
SII System Interconnection Interface (MIA)
SILS Standard for Interoperable LAN Security
SIMNET Simulation Network (US DoD)
SINCGARS Single-Channel Ground/Air Radio System (US DoD)
SIO Security Information Object (ISO SC27)
SIR Systeme d'Information Regimentaire (France)
SIS Standardiseringskommisionen i Sverige (Sweden)
SITPRO Simplified Trade Procedures
SM System Manager
SMA Systems Management Architecture (ISO)
SMCS System Management and Control System (Canada)
SMDS Switched Multimegabit Data Service
SMF System Management Facility (ATCCIS); System Management Function (ISO)
SMFA Systems Management Functional Area
SMI Structure of Management Information (OSI)
SMP System Management Protocol
SMPTE Society of Motion Picture and Television Engineers
SMS Swedish Mechanical Standardization; Subsystem Management Service (OSF's DME)
SMSL Standard Multimedia Scripting Language
SMT Station Management (FDDI)
SMTP Simple Mail Transfer Protocol (US DoD)
SN Subnetwork
SNA System Network Architecture (IBM)
SNARE Subnetwork Address Resolution Entity
SNC Special Network Concentrator (Germany)
SNDCF Subnetwork-Dependent Convergence Function
SNDCP Subnetwork Dependent Convergence Protocol (OSI Network Layer)
SNE Special Network Exchange (Germany)
SNES Special Network Exchange-Small (Germany)
SNI Simple Network Interface (IEEE)
SNICP Subnetwork Independent Convergence Protocol (OSI Network Layer)
SNMP Simple Network Management Protocol (Internet)
SNO Special Network Operations and Maintenance (O&M) (center) (Germany)
SNPA Subnetwork Point of Attachment
SNV Swiss Association for Standardization
SOGITS Senior Official Group for Information Technology Standardization (CEC)
SOGT Senior Official Group on Telecommunications (CEC)
SOM System Object Model
SOSTA Stand-Off Surveillance, Target, and Acquisition
SOTAS Stand-Off Target Acquisition System (US)
SP Security Protocol (SDNS); Spain
SPACECOM Space Command
SPAG Standards Promotion and Applications Group
SPARC Standards and Planning Requirements Committee
SPDL Standard Page Description Language
SPI Standard Programmatic Interface (SC21)
SPX Sequence Packet Exchange (Internet)
SQL/MM SQL for Multimedia and Application Packages
SRT Source Routing Transparent (LAN Bridging)
SSDB Standard Simulation Data Base
SSI System Software Interface
SSP Subnetwork Specific Protocol (Network Layer)
SSS Side-Scan Sonar (Distribution); System Segment Specification
STACCON Italian Army tactical CCIS (QIP)
STACCS Standard Theater Army Command and Control System (see AGCCS)
STAMINA Standard Automated Message Processing Interface for NATO's ACCISs
STANAG NATO Standardization Agreement
STC SHAPE Technical Centre
STD Standard
STDL Structured Transaction Definition Language (MIA)
STDN Strategic-Tactical Data Network (US DoD interoperability demonstration activity)
STE Signalling Terminal

STEI Service Technique de l'Electronique et de l'Informatique (France)
STEP Standard for the Exchange of Product Model Data
STL Standard Text Language
STM Synchronous Transfer Mode (SONET level)
STN Switched Telephone Network
STP Shielded Twisted Pair (cable)
STR Strategic (standard)
STRADIS Structured Analysis, Design and Implementation of Information Systems
STRIDA Systeme de Traitement et de Representation des Informations de Defense Aerienne (FR)
STS Synchronous Transport Signal (SONET level)
SUCOC Succession of Command
SUMM Semantic Unification Meta Model (IRDS)
SVC Stored Video Camera
SVR4 System V Release 4 (AT&T and BSD UNIX)
SVID System V Interface Definition (AT&T UNIX)
SWG Special Working Group (ISO JTC1)
SWG-CA Special Working Group on Conformity Assessment (JTC1)
SWG-EDI Special Working Group on Electronic Data Interchange
SWG-MF Special Working Group on Modelling Facilities (JTC1)
Synch Synchronous; Synchronized
SYSCOM System Control and Management (ZODIAC, The Netherlands)

T transport profile class providing COTS
TAC Tactical; Tactical Communications Protocol
TACFIRE Tactical Fire Direction System
TACS Tactical Air Control System (US Air Force)
TACSATCOM Tactical Satellite Communications
TADIL Tactical Digital Information Link
TADIXS Tactical Information Exchange System (US Navy)
TADKOM Norwegian tactical area communications system
TAOM Tactical Air Operations Module (US DoD)
TARE Telegraph Automated Routing Equipment
TASDAC Tactical Secure Data Communications (US Air Force)
TAWP Tactical Air Working Party (MAS Air Board, NATO)
TBD To Be Determined
TBITS Treasury Board Information Technology Standard (Canada)
TBM Tactical Battle Management (US DoD)
TC Transport Connections; Technical Committee (ISO)
TCA Telecommunications Association
TCAC Technical Control and Analysis Center
TCC Time-Critical Communications
TCCA Time-Critical Communications Architecture
TCCCS Tactical Command Control Communications System (Canada)
TCCS Time-Critical Communications System
TCDN Tactical Communications Distribution Node (US Marine Corps)
TCG Technical Coordination Group (CNSI)
TCIS Technical Common Interface Standards (TSGCE SG9)
TCOS Technical Committee on Operating Systems (IEEE)
TCP Transmission Control Protocol (US DoD)
TCP/IP Transmission Control Protocol/Internet Protocol
TCS Trusted Communications Sublayer (SANISI)
TCSEC Trusted Computer System Evaluation Criteria
TCSS Telecommunications Systems Standards (US DoD)
TCT Tactical Computer Terminal
TCU Transportable Computer Unit (US Army); Terminal Control Unit (packet radio)
TDC Time Dispersal Coding
TDI Trusted Database Interpretation
TDM Time Division Multiplexing
TDN Trunk Distribution Network (Canada)
TDP Technology Demonstrator Programme (UK)
TEI Terminal Endpoint Identifier (LAPD)
TEK Traffic Encryption Key
TELNET Telecommunications Network
Telcos Telecommunications Service Provider
TEM Terrain Evaluation Module (US Army)
TEN Tactical Extension Node (Canada)
TF Transfer Facility (ATCCIS)
TFA Transparent File Access (POSIX)
TGA Targa Image Format
TGRM Technical Group on Reference Models (ECMA)
THN Territorial Host Nation
TIDP Technical Interface Design Plan
TIFF Tag Image File Format
TLI Transport Library Interface; Transport Layer Interface
TLSP Transport Layer Security Protocol
TLV Tag-Length-Value
TM Technical Management; Technical Memorandum; Terminal Management
TMD Terminal Management Domain (TM)
TMHS Tactical Message Handling System (Canada)
TMN Telecommunication Management Network
TMP Test Management Protocol (TP)
TMS Tactical Message Switch (Norway)
TN Technical Note (STC)
TNI Trusted Network Interpretation
TNN Trunk Node Network
TOP Technical and Office Protocol
TOR Terms of Reference
TP Transaction Processing (OSI); Transport Protocol (OSI)
TP4 Transmission Protocol 4
TPDU Transport Protocol Data Unit (OSI)
TPI Transport Layer Protocol Interface

TPN Tactical Packet Network (US Army)
TPSUI Transaction Processing Service User Invocation
TR Technical Report (ISO)
TRAS Tactical Radio Access System (Norway)
TRI-MNC Tri-Major NATO Commanders' Command and Control Plan
TRI-TAC Joint Tactical Communications Program (US DoD)
TRM Technical Reference Model (US DoD)
TRP Technical Reinvestment Project
TRR Tactical Multi-Role Radio (Norway)
TS Transport Service (OSI); Telecommunication Standardization Sector (ITU)
TSA Time Synchronization Agent
TSAG Telecommunication
TSAP Transport Service Access Point
TSDN Transfer Syntax Description Notation (ASC X3T2)
TSG Technical Study Group (ISO/IEC JTC1)
TSGCE Tri-Service Group on Communications and Electronics (NATO) (formerly TSGCEE)
TSS Time Synchronization Service
TSSTP Test Suite Structures and Test Purposes
TTA Telecommunications Technology Association (Korea)
TTC Telecommunications Technology Committee (Japan)
TTCN Tree and Tabular Combined Notation (ISO)
TTGC Tactical Terminal System (France)
TTL Time to Live (XTP)
TTY Teletype
TUA Time User Agent
TUBA TCP/User Datagram Protocol (UDP) with Big Addresses
TWG Technical Working Group
TXI X/Open Transport Interface

U transport profile class providing CLTS
UA User Agent (MHS)
UAV Unmanned Aerial Vehicle
UCCS USAREUR Command Center System (US Army)
UCS Universal Coded Character Set (ISO)
UDO User Descriptor Object (TM)
UDP User Datagram Protocol
UDT Unstructured Data Transfer
UDWP Underwater Diving Working Party (MAS - Navy Board, NATO)
UER Union Europeenne de Radiodiffusion (European Union on Radio Broadcasting)
UHF Ultra High Frequency
UI UNIX International
UIDL User Interface Definition Language
UIL User Interface Language
UIMS User Interface Management System
UISRM User Interface System Reference Model
UIT Union Internationale des Telecommunications (CCITT)
UK United Kingdom
ULA Upper Layer Architecture (OSI)
ULTDS Unit Level Tactical Data Switch
UN United Nations
Unsynch Unsynchronized
UOD Universe of Discourse
UOF Unit of Functionality (TR 10000-3)
URSI International Union of Radio Science
USACOM US Atlantic Command
USAFGWS United States Air Force Global Weather Service
USAREUR US Army in Europe
USGS US Geological Survey
USL UNIX Systems Laboratories (formerly AT&T, now a wholly owned subsidiary of Novell, Inc.)
USPACOM US Pacific Command
US-SIOP-ESI United States - Single Integrated Operation Plan - Extremely Sensitive Information
USSPACECOM US Space Command
UTACCS USAREUR Tactical Command and Control System (now STACCS; see also AGCCS)
UTC Coordinated Universal Time
UTE Union Technique de l'Electricite (France)
UTP Unshielded Twisted Pair (cable)

VC Virtual Circuit
VCC Verification Coordinating Committee (NAC in NATO)
VCI Virtual Channel Identifier (ATM)
VDI Virtual Device Interface
VDM-SL Vienna Development Method-Specification Language
VDT Visual Display Terminal
VDU Visual Display Unit
VEX Video Extension to X
VFUIF Voice/Fax User Interface Forum
VIM Vendor Independent Messaging (Lotus Development Corp.)
VMD Virtual Manufacturing Device
VMEbus Versa Module Europe Bus
VMF Variable Message Format
VMUIF Voice Messaging User Interface Forum
VPF Vector Product Format (DMA)
VPI Virtual Path Identifier (ATM)
VPS Vector Product Standard
VSAT Very Small Aperture Terminal
VSLAN Verdix Secure LAN
VSR Validation Summary Reports (SQL)
VT Virtual Terminal (OSI Layer 7)
VTC Video Teleconferencing
VTE Virtual Terminal Environment
VTP Virtual Terminal Protocol
VXI Extensions for Instrumentation

W	Workstation
WAM	WWMCCS Automated Data Processing (ADP) Modernization
WAN	Wide Area Network
WAS	Wide Area Subsystem
WAVELL	UK Army CCIS
WD	Working Draft
WDAD	Working Draft Addendum (ISO)
WDAM	Working Draft Amendment (ISO)
WDB	World Data Bank
WDISP	Working Draft International Standardized Profile
WDS	WRRE Demonstrator System
WES	WAVELL Enhancement System
WG	Working Group
WHIDDS	War Headquarters Information Dissemination and Display System
WHQs	War Headquarters
WIMP	Windows-Icons-Menus-Pointer (user interface)
WIN	WWMCCS Intercomputer Network
WIS	WWMCCS Information System
WOSA	Windows Open Services Architecture (Microsoft)
WP	Working Paper (ATCCIS); Working Party
WRRE	WAVELL Risk Reduction Exercise
WS	Work Station
WSF	Workstation Function
WTSC	World Telecommunication Standardization Conference (formerly CCITT Plenary Assembly)
WWMCCS	Worldwide Military Command and Control System
X11	X-Windows, Version 11
XALS	Extended ALS (OSI)
XAP	X/Open ACSE/Presentation API
XAPIA	X.400 Application Programming Interface Association
XDS	X/Open Directory Service
XDSX	X/Open Directory Services API
XFTAM	X/Open FTAM API
XIA	X Industry Association
XID	Exchange Identification
XIE	X-Image Extension
XLib	X Library
XOM	OSI Object Management API
X/Open	UNIX Open Application Group (consortium)
XPG	X/Open Portability Guide
XPG3	Third Edition of the X/Open Portability Guide
XPG4	Fourth Edition of the X/Open Portability Guide
XRUA	X-Window-Based Remote User Agent
XSI	X/Open System Interfaces
XT	X Toolkit Intrinsics
XTIX	X/Open Transport Interface API
XTP	Xpress Transfer Protocol
XTV	X Teleconferencing and Viewing
XVS	X/Open System V Specification
XVT	Extensible Virtual Toolkit
ZODIAC	Zone Digital Automatic Cryptographic (The Netherlands)

(This page intentionally left blank.)

INDEX

INDEX